The Impact of Digital Surveillance on Freedom of Expression in the Americas

IACHR Inter-American Commission on Human Rights

RFOE SPECIAL RAPPORTEUR FOR FREEDOM OF EXPRESSION

OEA/Ser.L/V/II
CIDH/RELE/
INF.33/25
September 2025
Original in English

The Impact of Digital Surveillance on Freedom of Expression in the Americas

Special Rapporteurship for Freedom of Expression of the
Inter-American Commission on Human Rights

Pedro Vaca Villarreal
Special Rapporteur for Freedom of Expression

OAS

IACHR Inter-American Commission on Human Rights | RFOE SPECIAL RAPPORTEUR FOR FREEDOM OF EXPRESSION

OAS Cataloging-in-Publication

Data

Inter-American Commission on Human Rights. Office of the Special Rapporteur for Freedom of Expression.

Informe especial sobre la situación de la libertad de expresión en Chile: 2024 / Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos.

v. ; cm. (OAS. Documentos oficiales ; OEA/Ser.L/V/II)

ISBN 978-0-8270-8040-9

1. Freedom of expression--America. 2. Electronic surveillance--America. 3. Privacy, Right of--America. 4. Freedom of information--America. 5. Human rights--America. I. Vaca Villarreal, Pedro. II. Title. III. Series.

OEA/Ser.L/V/II CIDH/RELE/INF.33/25

Inter-American Commission on Human Rights

Members
José Luis Caballero Ochoa
Andrea Pochak
Arif Bulkan
Roberta Clarke
Carlos Bernal Pulido
Edgar Stuardo Ralón Orellana
Gloria Monique de Mees

Executive Secretary
Tania Renaum Panszi

Chief of Staff
Patricia Colchero Aragonés

Assistant Executive Secretary for Monitoring, Promotion and Technical Cooperation
María Claudia Pulido Escobar

Assistant Executive Secretary for the Petitions and Cases System
Jorge Meza Flores

Special Rapporteur for Freedom of Expression
Pedro Vaca Villarreal

Special Rapporteur on Economic, Social, Cultural, and Environmental Rights
Javier Palummo Lantes

This report was approved on 7 September 2025.

TABLE OF CONTENTS

I. INTRODUCTION 2
A. Background and purpose of the report 2
B. Methodology and structure 2
II. DIGITAL SURVEILLANCE IN THE AMERICAS 5
A. Surveillance technologies and documented applications 5
1. Spyware 5
a. Mexico 5
b. El Salvador 7
c. Dominican Republic 8
d. Colombia 8
e. Other cases in the region 8
f. Transnational digital repression 9
2. Online profiling and cyber patrolling 9
3. Facial recognition and biometrics 10
4. Geolocation tracking and SS7 exploitation 11
5. Network monitoring, advertising intelligence (AdInt), data brokers, and AI governance frameworks 13
6. Migration-related surveillance 16
B. Normalization of surveillance 20
C. Human rights impacts of surveillance abuses 22
1. Surveillance generates widespread chilling effects on freedoms of expression, peaceful assembly, association, movement and thought 24
2. Surveillance undermines human rights defense and investigative and critical journalism 25
3. Surveillance results in significant intersectional and gender-based harms 31
4. Surveillance impunity creates a state of continuous violation of the rights of targeted individuals 36
III. REGIONAL AND INTERNATIONAL LEGAL FRAMEWORK 43
IV. PROGRESS AND GOOD PRACTICE 54
V. LEGITIMACY IN THE SURVEILLED WORLD: DISTINGUISHING LEGITIMATE FROM INDISCRIMINATE USE OF SURVEILLANCE TECHNOLOGIES 58
A. The Inter-American Court's approach to surveillance 59
1. Fulfillment of the international human rights law requirements of legality, legitimate aim, suitability, necessity, and proportionality 59
2. A robust domestic system for control of the use of surveillance technologies 60
3. An independent civilian oversight authority 61
4. A mechanism for remedy and reparation in the event of surveillance abuse 63
B. Guardrails around private sector participation in state surveillance 64
VI. CONCLUSIONS AND RECOMMENDATIONS 69

INTRODUCTION

A. Background and purpose of the report

1. Well into the third decade of the 21st century, it is widely documented and understood that states' use of advanced digital surveillance technologies presents an existential threat to human rights, in the Americas and beyond. Counter-terrorism initiatives, law enforcement alarm over "going dark" as an insecure digital ecosystem incorporates enhanced encryption, and other efforts to address criminal activity and national security threats have all propelled surveillance capabilities. State architectures of compliance with international human rights law in the use of such tools, however, have failed to keep up with technological advances. Invasive digital surveillance techniques – deemed *exceptional* under international human rights law frameworks due to their impact on the rights to freedom of expression, privacy, and a host of other rights – are increasingly *normalized* in practice and public perception. Recalibration is long overdue, yet state actors have not yet mustered the political will to tackle the root of their surveillance excess.

2. The human rights impacts of digital surveillance are severe and widespread. In the Americas alone, the Office of the Special Rapporteur (SRFOE) of the Inter-American Commission on Human Rights (IACHR) has observed the targeting of human rights defenders, environmental activists, journalists, lawyers, opposition leaders, and public health experts. These individuals have felt their privacy violated and have no means of knowing what information was taken from them, or when and how it will be used against them. In many instances, digital surveillance is one component of ongoing repression and persecution, and in some cases has preceded physical harm. The effects are felt not only by the targeted individuals whose rights are violated, but by their families and contacts, and by society at large, as human rights defense, media freedom, public discourse and engagement, and democracy itself are undermined. Predictably, surveillance abuses have fundamentally altered the risk exposure societies face, with the commercialization of tools that facilitate extraterritorial targeting of investigative journalists, diaspora communities, and even state officials.

3. The SRFOE has prepared this thematic report on the use of digital surveillance technologies in the Americas to assess the human rights impacts of surveillance in this region; consider the legal frameworks and standards applicable to surveillance practice within the OAS, including the jurisprudence of the Inter-American Court of Human Rights; and highlight the key policy issues and practical gaps that remain in achieving compliance with international human rights law as it concerns digital surveillance. The report builds on the monumental efforts and achievements of civil society, journalists, independent experts, and others who have worked for many years to call attention to digital surveillance technologies and abuses. The report recognizes as well the existing initiatives of states and the private sector to bring more accountability to the commercial surveillance market.

B. Methodology and structure

4. This report was prepared using a mixed methodology that combines various primary and secondary sources of information, in order to obtain a comprehensive understanding of the impact of digital surveillance on freedom of expression in the Americas.

5. Regarding ***primary sources***, the SRFOE used multiple information gathering mechanisms:

5.1. It obtained information from OAS Member States, based on a request for information, as part of its monitoring mandate, in order to obtain official data and learn about laws and measures implemented in relation to digital surveillance.[1]

5.2. It received written input through an open public consultation addressed to civil society organizations, journalists, media outlets, human rights defenders, researchers, academics, and other stakeholders.[2]

5.3. It conducted interviews with 16 individuals with expertise concerning digital surveillance, including representatives of civil society organizations and academic institutions.[3]

5.4. It also conducted interviews with 28 individuals whose devices were documented to have been infected with Pegasus spyware.[4]

5.5. It also gathered input during a peer review of the initial draft of this report, held on April 24, 2025, in Washington, D.C.

5.6. It also drew upon relevant information from public hearings held before the IACHR, including "Mexico: Protection of Human Rights Defenders and Journalists" (189th Period of Sessions, February 28, 2024); "Human rights and the use of facial recognition technologies in Brazil" (187th Period of Sessions, July 11, 2023); "The human rights situation in the context of cyber-surveillance in El Salvador" (183rd Period of Sessions, March 16, 2022); "Use of surveillance technologies and their impact on freedom of expression in the context of the pandemic in the region" (181st Period of Sessions, October 27, 2021); and "Protection of human rights of defenders and communicators in Mexico" (180th Period of Sessions, July 1, 2021).

6. Regarding ***secondary sources***, the following were considered: (a) reports, guides, and other relevant documents from civil society organizations; (b) information from official sources; (c) reports, resolutions, and statements from international organizations; (d) information from the media; and (e) academic research.

7. This report is organized into six chapters. Chapter I presents the introduction, which sets out the background, purpose, and methodology of the report. Chapter II assesses the experience of digital surveillance in the Americas, providing detail on the surveillance technologies deployed, highlighting the increasing normalization of surveillance in public life, and examining the resulting human rights impacts. Chapter III explores the applicable legal framework, covering relevant international instruments, State obligations in deploying surveillance, and the specific rights and standards implicated by the use of surveillance technologies. Chapter IV lays out good practices and progress achieved thus far in addressing the human rights impacts of digital surveillance, and notes remaining gaps. Chapter V applies the standards laid out in the Inter-American Court of Human Rights' 2024 decision in the *Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia*, and considers the factors essential to establishing legitimate use by States of digital surveillance technologies. Finally, Chapter VI presents conclusions and recommendations for OAS Member States and the international community to address this issue.

[1] The Office of the Special Rapporteur for Freedom of Expression (SRFOE) received written inputs from the OAS Permanent Missions of Argentina, Ecuador, and Mexico.

[2] The SRFOE received written inputs from Article 19; Instituto de Democracia y Derechos Humanos de la Pontificia; Universidad Católica del Perú; Fundación Ciudadanía y Desarrollo (FCD); Media Legal Defence Initiative; R3D; Association for Progressive Communications (APC); Derechos Digitales; El Veinte; Amnesty International, Americas Regional Office; Access Now; Karisma Foundation, as well as independent experts and academics.

[3] The SRFOE held interviews with Access Now; Electronic Frontier Foundation (EFF); SocialTIC; Amnesty International's Security Lab; Knight First Amendment Institute; R3D, as well as independent experts and academics.

[4] The names of individuals interviewed by the SRFOE are withheld to maintain confidentiality.

8. The SRFOE emphasizes that the cases and countries discussed in this report are illustrative of regional patterns rather than exhaustive, recognizing that surveillance abuses may be occurring in additional countries beyond those specifically examined herein.

I. DIGITAL SURVEILLANCE IN THE AMERICAS

9. The experience of digital surveillance in the Americas elucidates the risks of surveillance technology and its long-term human rights impacts and policy implications. The region has grappled for decades with surveillance abuses,[5] including some of the earliest documented cases of the deployment of NSO Group's Pegasus spyware against journalists and civil society. This chapter explores documented cases and reports indicating that State authorities have employed a wide spectrum of surveillance tactics in the region, and how surveillance practices continue to evolve. It then examines the troubling trend toward normalization of surveillance in the Americas, and the human rights impacts of digital surveillance.

A. Surveillance technologies and documented applications

1. Spyware

10. The use of targeted invasive surveillance technology, or spyware, in the region is of particular concern, given the far-reaching human rights implications of the total device access provided by commercial spyware. In addition to states' own deployment of spyware tools, cases have also emerged of politically motivated *extraterritorial* targeting within the region, which has highlighted the importance of defending against the malicious use of such tools by external actors.

a. Mexico

11. Mexico was one of the first countries where the IACHR and its Special Rapporteurship documented the use of NSO Group's Pegasus spyware[6]. The research and reporting around spyware abuse in Mexico has brought to light a wide range of constituencies targeted with invasive surveillance tools for political advantage or to prevent accountability of powerful interests. Research from civil society organizations ARTICLE 19, Citizen Lab, R3D, and SocialTIC documented the use of NSO Group's Pegasus spyware during the 2012-2018 presidential administration against at least 25 targets[7], including: anti-corruption advocates from Mexicans Against Corruption and Impunity (MCCI) and the Mexican Institute for Competitiveness (IMCO)[8]; human rights defenders, including members of the Miguel Agustín Pro Juárez Human Rights Center AC (Centro Prodh)[9]; journalists from media outlets, as well as family members of journalists[10]; lawyers representing families of victims in high-profile cases[11]; members of the Interdisciplinary Group of Independent Experts (GIEI) established

[5] See, e.g., University of California, 'Discredit, disrupt, and destroy': FBI records acquired by the Library reveal violent surveillance of Black leaders, civil rights organizations, January 18, 2021; Open Canada, Surveillance in Canada: Who are the watchers?, July 6, 2017; Canada's History, Spying on Canadians, November 14, 2018; Eduardo Beroni and Collin Kurre, "Surveillance and Privacy Protection in Latin America: Examples, Principles, and Suggestions", in Fred H. Cate, and James X. Dempsey (eds), *Bulk Collection: Systematic Government Access to Private-Sector Data*, Oxford Academic, 19 Oct. 2017; Privacy International and Asociación por los Derechos Civiles (ADC), Who's watching the Watchers? A comparave study of intelligence organisaons oversight mechanisms, May 2014.

[6] The Citizen Lab, The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender, August 24, 2016.

[7] See The Citizen Lab, Reckless VII: Wife of Journalist Slain in Cartel-Linked Killing Targeted with NSO Group's Spyware, March 20, 2019; Information submitted by R3D in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 2-3; Information submitted by Article 19 Office for Mexico and Central America in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 3.

[8] The Citizen Lab, Reckless V: Director of Mexican Anti-Corruption Group Targeted with NSO Group's Spyware, August 30, 2017.

[9] R3D, Ejército mexicano espió con Pegasus a dos personas defensoras de derechos humanos del Centro Prodh, April 18, 2023; Centro Prodh, Espionaje al Centro Prodh.

[10] The Citizen Lab, Reckless VI: Mexican Journalists Investigating Cartels Targeted with NSO Spyware Following Assassination of Colleague, November 27, 2018; R3D and Privacy International, The right to privacy in Mexico: Alternative report to the Human Rights Committee, 127th Session - Mexico, September 2019.

[11] The Citizen Lab, Reckless IV: Lawyers for Murdered Mexican Women's Families Targeted with NSO Spyware, August 2, 2017.

by the IACHR to investigate the 2014 mass disappearance in Iguala of 43 students from Ayotzinapa Rural Teachers' College[12]; public health researchers and advocates working on issues such as national health policies, including individuals from the Instituto Nacional de Salud Pública, consumer rights organizations and health advocacy coalitions[13]; legislators and politicians[14].

12. In 2021, the Pegasus Project[15] revealed a leak of more than 50,000 phone numbers selected as potential Pegasus targets; 15,000 of those bore the country code for Mexico.[16] Numbers included human rights defenders and relatives of the 43 disappeared Ayotzinapa Rural Teachers College students, as well as public officials.[17] The Pegasus Project further reported that at least 25 journalists in Mexico were targeted with Pegasus spyware over a two-year period,[18] including a journalist whose phone was selected for targeting in the weeks before his killing in 2017.[19]

13. More cases of spyware abuse were documented between 2018-2024. It is noteworthy that the additional spyware cases that have come to light appear to have a connection with the targets' work concerning human rights abuses by the military, including the involvement of the military in the mass disappearance of the Ayotzinapa students.[20]

14. All of these incidents demonstrate the reported illegitimate use of spyware over many years in Mexico, whether that be to obtain information about political opposition or social movements, or to prevent accountability for human rights abuses. Journalistic investigations, requests for access to information, and document leaks such as those of the Guacamaya collective indicate that Pegasus spyware was allegedly acquired and/or used by state entities including the National Defense Secretariat, the Military Intelligence Center, the Center for Intelligence and National Security, and the Attorney General's Office.[21] According to available information, in Mexico, the military does not have legal authority to intercept the private communications of civilians.[22]

15. While NSO Group's Pegasus is the most prominent spyware tool utilized in Mexico, various other commercial spyware tools are known to have been acquired at different points in time from multiple

[12] The Citizen Lab, Reckless III: Investigation Into Mexican Mass Disappearance Targeted with NSO Spyware, July 10, 2017.
[13] The Citizen Lab, Bitter Sweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links, February 11, 2017.
[14] The Citizen Lab, Reckless Redux: Senior Mexican Legislators and Politicians Targeted with NSO Spyware, June 29, 2017.
[15] A collaboration of more than 80 journalists from 17 media organizations in 10 countries, coordinated by Forbidden Stories with Amnesty International as technical partner; Information submitted by Amnesty International, Americas Regional Office, in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 1.
[16] Information submitted by R3D in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 3.
[17] Information submitted by R3D in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 3.
[18] Information submitted by Amnesty International, Americas Regional Office, in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 1; Deutsche Welle (DW), Pegasus spyware: Mexico one of the biggest targets, July 22, 2021;
[19] Forbidden Stories, Pegasus: The new global weapon for silencing journalists, July 18, 2021.
[20] Information submitted by R3D in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 3; see also The Citizen Lab, 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; Reuters, Mexican armed forces were complicit in students' disappearance, new report finds, July 25, 2023; Human Rights Watch, Ayotzinapa, Mexico's Army, and López Obrador's Silence, September 26, 2023; ARTICLE 19, Espionaje contra Camilo Vicente Ovalle expone sabotaje militar al esclarecimiento de abusos de la Guerra Sucia, June 5, 2023; The New York Times, He Was Investigating Mexico's Military. Then the Spying Began, May 22, 2023; The New York Times, Pegasus spyware reaches into Mexican president's inner circle, May 25, 2023; R3D, ARTICLE 19 Mexico and Central America, and SocialTIC, "Ejército Espía" Report, 2022; ARTICLE 19, Mexico: Army used Pegasus to spy on human rights defender Raymundo Ramos, March 07, 2023.
[21] Information submitted by R3D in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 8-9.
[22] Information submitted by R3D in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 9.

international vendors.[23] According to the information received by this Office, an extensive network of intermediary companies have reportedly facilitated contracts between state entities and surveillance technology providers.[24]

b. El Salvador

16. In another example of widespread targeting of journalists, human rights defenders, and others, investigations confirmed the use in El Salvador of NSO Group's Pegasus spyware. A number of Salvadorans, including journalists and politicians, received an Apple threat notification warning of targeting by state-sponsored attackers in November 2021.[25] A subsequent investigation undertaken by Citizen Lab and Access Now, in collaboration with Frontline Defenders, SocialTIC, and Fundación Acceso and with independent review of technical data by Amnesty International's Security Lab, confirmed that the mobile devices of individuals were infected with NSO Group's Pegasus spyware between July 2020 and November 2021, including journalists and staff from *El Faro* newspaper, *GatoEncerrado*, *El Diario de Hoy*, *Diario El Mundo*, *La Prensa Gráfica*, *Revista Disruptiva*, as well as independent journalists, economists and columnists for independent media, and staff members from civil society organizations including Cristosal and Fundación DTJ.[26] The IACHR and the Regional Office of the United Nations High Commissioner for Human Rights (OHCHR) for Central America and Dominican Republic expressed their deep concern about this evidence of illegal surveillance and urged the State to effectively and impartially investigate these allegations.[27]

17. The IACHR had granted precautionary measures for 34 individuals who work at *El Faro* newspaper in February 2021, recognizing that their "right to life and personal integrity… are in a serious and urgent situation" after they were "subjected to constant stigmatization, harassment, criminalization and threats from the government."[28] The IACHR requested, inter alia, that the state of El Salvador "take the necessary measures so that the beneficiaries can carry out their journalistic activities in exercise of their right to freedom of expression, without being subjected to acts of intimidation, threats and harassment."[29] Yet the devices of many of these individuals were infected with Pegasus in or around that period of time. In April 2023, *El Faro* moved its legal and administrative operations to Costa Rica, forced into partial exile in order to continue its operations.[30]

[23] This would include Gamma International's FinFisher, Hacking Team's Galileo Remote Control System, and QuaDream spyware. Information submitted by R3D in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 5-6.

[24] Information submitted by R3D in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 33-37.

[25] Information submitted by Access Now in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 1.

[26] The Citizen Lab, Project Torogoz: Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware, January 2022.

[27] IACHR, IACHR, Its Special Rapporteurship for Freedom of Expression and OHCHR Are Concerned About Evidence of the Use of Pegasus Malware to Spy on Journalists and Civil Society Organizations in El Salvador, Press Release 022/22, January 31, 2022.

[28] IACHR, Resolution 12/2021, Precautionary Measure No. 1051-20, 34 identified members of the digital newspaper "El Faro" regarding El Salvador, February 4, 2021, paras. 3 and 5; See also IACHR, Press Release No. 160/22, IACHR Grants Follow-Up Resolution Concerning Precautionary Measure for Members of Salvadoran Newspaper El Faro, July 13, 2022.

[29] IACHR, Resolution 12/2021, Precautionary Measure No. 1051-20, 34 identified members of the digital newspaper "El Faro" regarding El Salvador, February 4, 2021, para. 53.

[30] Information submitted by Access Now in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 4.

c. Dominican Republic

18. In the Dominican Republic, an investigative journalist was targeted and her device was infected with NSO Group's Pegasus spyware three times between 2020 and 2021. The journalist's work focused on issues of corruption and impunity.[31] While this was the first documented instance of a Pegasus infection, interviews conducted in 2022 and 2023 by Amnesty International with journalists and human rights defenders in the country indicated that "nearly all . . . suspected they had been targeted for surveillance because of their work."[32] Additionally, in 2023, political leaders reported receiving Apple notifications of state-sponsored attacks against their iPhones.[33]

d. Colombia

19. According to public information, in 2024 Colombian President stated that the country's police intelligence directorate had purchased Pegasus spyware from NSO Group for a total of US$11 million, and indicated the spyware may have been used by the prior administration to surveil political opposition. He ordered an investigation into the matter, and acknowledged that the spyware expenditure was not reflected in official budget records.[34] It was later reported that the U.S. had financed the purchase of the spyware for the purpose of combating drug trafficking.[35]

20. Additionally, media reporting in 2020 revealed the use by the Colombian Military Forces of an intrusion technology referred to as "Invisible Man" to surveil public officials and human rights defenders.[36] A 2021 Meta incident report noted the company had detected users of Cytrox's Predator spyware in Colombia.[37]

21. The Inter-American Court of Human Rights has found that Colombian authorities conducted extensive digital surveillance operations against human rights defenders and lawyers. The 2024 decision of the Court in the case brought by the Jose Alvear Restrepo Lawyers Collective (CAJAR) against the state of Colombia – discussed further below – confirmed that the members of the collective were subjected to years of surveillance in multiple forms, including interception of private communications, alongside numerous other rights abuses.[38]

e. Other cases in the region

22. Brazil has reportedly previously explored acquiring Pegasus software during the 2019-2021 administration, and the Brazilian Federal Police reportedly purchased spyware from the Italian

[31] Information submitted by Amnesty International, Americas Regional Office, in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 3.
[32] Information submitted by Amnesty International, Americas Regional Office, in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 4.
[33] Information submitted by an independent expert in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, July 2024, p. 5; Diario Libre, José Dantés y Juan Ariel Jiménez denuncian intento de hackeo a sus celulares para "instalar Pegasus", October 30, 2023.
[34] BBC News, Colombia to investigate police purchase of Pegasus spyware, September 5, 2024.
[35] Barron's, Washington Financed Colombia's Purchase Of Pegasus Spy Software, November 8, 2024; El Tiempo, Exclusivo: 'Queremos dejar muy claro que fue EE. UU. quien financió compra de Pegasus en Colombia con recursos lícitos', November 7, 2024.
[36] Information submitted by Fundación Karisma in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 6.
[37] Information submitted by an independent expert in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, July 2024, p. 4; Mike Dvilyanski, David Agranovich, Nathaniel Gleicher, Threat Report on the Surveillance-for-Hire Industry, December 16, 2021.
[38] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections, Merits, Reparations and Costs. October 18, 2023. Series C No. 506, para. D.4.2.

company Hacking Team (now Memento Labs).[39] The Panamanian government is alleged to have acquired Pegasus as well in 2015.[40] In Chile, an investigation is underway regarding the use by Chile's national police force, the Carabineros, of an undetermined spyware in 2017.[41]

f. Transnational digital repression

23. Transnational repression is defined by Freedom House as "governments reaching across borders to silence dissent among diasporas and exiles, including through assassinations, illegal deportations, abductions, digital threats, Interpol abuse, and family intimidation."[42] The concept of transnational *digital* repression is defined by Citizen Lab as government use of "digital technologies to surveil, intimidate, and silence exiled and diaspora communities."[43] It provides states extraterritorial reach, allowing them to control political opposition and dissent beyond their own jurisdictions. Based on reports received, spyware was utilized as a tool of transnational digital repression to surveil individuals in Canada and the U.S., including activists, human rights defenders, and family members of prominent dissidents.[44]

2. Online profiling and cyber patrolling

24. According to information received by the Special Rapporteurship, governments within the Americas have increasingly relied upon online profiling and so-called "cyber patrolling" to monitor and crack down on online activity critical of state authorities, using advanced open source intelligence tools in what amounts to a new form of mass surveillance.[45] For example, it has been reported that States have contracted private services to provide social media monitoring and characterize individual users according to their views of the state, measuring people's "acceptance of the government and its authorities, and designing strategies to ensure their positioning on social networks."[46] At the same time, a number of law enforcement and intelligence entities in the region have rolled out cyber patrolling frameworks to monitor users of digital platforms, and even engage with them through fake profiles, for the ostensible purpose of collecting information that will allow them to prevent, detect, and prosecute crime[47]. In practice, cyber patrolling has been used to target

[39] Information submitted by Association for Progressive Communications in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, pp. 12-13.

[40] Council of Europe, Report Pegasus and similar spyware and secret state surveillance, September 20, 2023, para. 13.

[41] Information submitted by an independent expert in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, July 2024, p. 4.

[42] Freedom House, Transnational Repression; see also Special Report: Unsafe in America: Transnational Repression in the United States, 2022.

[43] Citizen Lab, The Kingdom Came to Canada, October 1, 2018, at p. 1; see also Knight First Amendment Institute at Columbia University, Silenced by Surveillance: The Impacts of Digital Transnational Repression on Journalists, Human Rights Defenders, and Dissidents in Exile, February 18, 2025.

[44] Citizen Lab, The Kingdom Came to Canada, October 1, 2018; The Guardian, Hotel Rwanda activist's daughter placed under Pegasus surveillance, July 19, 2021; EFF, Kidane v. Ethiopia.

[45] Information submitted by Derechos Digitales in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024.

[46] Information submitted by Derechos Digitales in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 5-8; The Intercept Brasil, Governo Bolsonaro deturpou edital de Dilma para fichar 'detratores' na internet, July 7, 2021; Índice Derechos Digitales, Ciberpatrullaje de la Policía Nacional para identificar desinformación, July 7, 2023; Lucía Camacho Gutiérrez, Daniel Ospina Celis, Juan Carlos Upegui Mejía, Inteligencia estatal en internet y redes sociales: el caso colombiano, Dejusticia, December 2022.

[47] Derechos Digitales, Ciberpatrullaje: cuando vigilar se justifica en nombre de la seguridad, May 9, 2025; Chequeado, Ciberpatrullaje: qué dice el nuevo decreto y qué implican los cambios en la Policía Federal, June 19, 2025; Fundación Karisma, Cuando el estado vigila. Ciberpatrullaje y OSINT en Colombia, February 27, 2023; Electronic Frontier Foundation (EFF), The Battle for Communications Privacy in Latin America: 2021 in Review, December 27, 2021; Datysoc, Ciberpatrullaje: ampliación del informe y resultados del litigio sobre vigilancia policial en Internet, july 2024.

expression critical of the state, as well as "fake news" and disinformation.[48] Journalists and civil society have reported confirmed or suspected use of cyber patrolling in Argentina, Bolivia, Brazil, Colombia, Mexico, Paraguay, and Uruguay.[49]

25. Additionally, in Cuba and Venezuela, authorities have arrested a number of individuals for publishing critical content on social networks and other online platforms, suggesting systematic monitoring of digital activity.[50]

26. According to available information, various profiling and open source intelligence technologies have been utilized in some of these operations in the region. [51]

27. As noted by the NGO Derechos Digitales, these pervasive monitoring practices fundamentally reject the notion of privacy in the online environment and "place people in a state of continuous suspicion by their mere interaction on the Internet, which makes them potential targets of State surveillance and, therefore, subject to criminal proceedings."[52] The IACHR and this mandate have expressed particular concern about the use of profiling and cyber-patrolling in Venezuela following the 2024 presidential election, where such techniques have been used as a means of digital repression to crack down on protest and criticism of the government and the electoral process.[53]

3. Facial recognition and biometrics

28. According to information received by the Special Rapporteurship, states have reportedly used surveillance incorporating facial recognition or biometrics in various countries of the region.[54] Indiscriminate use of such tools in public areas constitutes a form of mass surveillance, raising questions around the necessity and proportionality of such measures, lack of adequate human rights assessments and safeguards, and the risk of false positives when used for policing, particularly given the documented racial bias of such tools.[55] Various international technology companies have reportedly supplied facial recognition and biometric technology in the region.[56]

---

[48] Information submitted by Derechos Digitales in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 11-20; Information submitted by Article 19 Office for Mexico and Central America in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 7; Information submitted by Fundación Karisma in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 1-2.

[49] Information submitted by Derechos Digitales in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024; Information submitted by an independent expert in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, July 2024, p. 3-4.

[50] Information submitted by an independent expert in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, July 2024, p. 3.

[51] This would include commercial intelligence software and social media monitoring platforms, such as HIWIRE software and UCINET. Information submitted by Derechos Digitales in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, 30 August 2024, p. 24-26.

[52] Information submitted by Derechos Digitales in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, 30 August 2024, p. 5.

[53] IACHR, Press Release No. R190/24, The SRFOE Alerts the International Community about Arbitrary Detention of Journalists and Criminalization of Dissent in Venezuela, August 23, 2024; IACHR, Press Release No. 184/24, IACHR and SRFOE condemn State terrorism practices in Venezuela, August 15, 2024.

[54] Information submitted by an independent expert in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, July 2024, p. 2-3; Access Now, Surveillance Tech in Latin America: Made Abroad, Deployed at Home, January 13, 2023; Chatham House, Regulating facial recognition in Latin America, November 11, 2022; Information submitted by Article 19 Office for Mexico and Central America in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 7.

[55] Joy Buolamwini, Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, 2018.

[56] Access Now, Surveillance Tech in Latin America, Made Abroad, Deployed at Home, August 2021, p. 4

29. In Argentina, the city of Buenos Aires implemented a city-wide video surveillance system reliant on facial recognition technology in 2019. The Court of Appeals of the City of Buenos Aires ruled use of the system unconstitutional in 2023, finding the system was implemented without proper controls. Its ruling highlighted the serious risks of the system, including "false positive" incidents in which innocent civilians were identified as criminals; apparent incorporation into the surveillance database of extensive personal data from the population; and improper use of the tool to monitor individuals not wanted for criminal activity.[57] The SRFOE welcomed this decision, "which protects citizens from potential violations of privacy rights and related rights. Real-time biometric recognition poses serious risks under international human rights law".[58]

30. The use of facial recognition surveillance technology in Brazil has raised warnings regarding racial bias.[59] During the 187th Period of Sessions of the IACHR, Brazilian civil society organizations drew attention to issues of racial profiling deepened by facial recognition technologies in public security, reporting various cases of wrongful detention of Black individuals due to the use of this technology and attributing responsibility to racial biases of public security authorities in data interpretation, as well as biases in programming and databases that feed facial recognition systems.[60] Facial recognition surveillance is deployed widely across Brazil. In 2023 it was reported that since 2019, 90% of the people arrested using facial recognition technology were black.[61] Data suggests enormous numbers of false positives, for example, an 81% rate of unjust arrests involving black individuals in the state of Rio de Janeiro in 2021.[62]

31. Based on available information, in the U.S., the expansive adoption of facial recognition surveillance technology by local police departments has reportedly resulted in widespread mass surveillance, raising concerns about potential impacts on the rights to privacy, equality, non-discrimination, and the freedoms of expression and association.[63] In 2022, Amnesty International documented that the New York Police Department's use of facial recognition disproportionately affected communities of color, particularly in neighborhoods previously subjected to aggressive stop-and-frisk practices, and has reinforced racially biased policing.[64] In some cases reliance by law enforcement on facial recognition has reportedly led to wrongful arrests.[65]

32. States have also deployed facial recognition and biometric technologies widely in migration-related surveillance, discussed further below in Section II.A.6.

4. Geolocation tracking and SS7 exploitation

33. Device-based location tracking poses growing challenges in the Americas, following a number of incidents of misuse by state authorities. Location data is highly sensitive as it paints a detailed

[57] Centro de Estudios Legales y Sociales, Confirman la inconstitucionalidad del uso del sistema de reconocimiento facial, April 29, 2023; Wired, The Twisted Eye in the Sky Over Buenos Aires, September 13, 2023.

[58] IACHR, Annual Report 2023, Office of the Special Rapporteur for Freedom of Expression Annual Report, OEA/Ser.L/V/II Doc. 386, December 6, 2023, paras. 106-107.

[59] IACHR, Hearing, Human rights and the use of facial recognition technologies in Brazil, 187th Period of Session, July 11, 2023.

[60] IACHR, Hearing, Human rights and the use of facial recognition technologies in Brazil, 187th Period of Session, July 11, 2023.

[61] Reuters, FEATURE-Brazil turns facial recognition on rioters despite racism fears, January 12, 2023.

[62] Aljazeera, Facial recognition surveillance in São Paulo could worsen racism, July 13, 2023.

[63] Amnesty International, USA: Facial Recognition Technology Reinforcing Racist Stop-and-Frisk Policing in New York – New Research, February 15, 2022; ACLU, Police Say a Simple Warning Will Prevent Face Recognition Wrongful Arrests. That's Just Not True, April 30, 2024.

[64] Information submitted by Amnesty International's Security Lab in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, May 2025; Amnesty International, USA: Facial Recognition Technology Reinforcing Racist Stop-and-Frisk Policing in New York – New Research, February 15, 2022; Amnesty International, Ban the scan.

[65] ACLU, Police Say a Simple Warning Will Prevent Face Recognition Wrongful Arrests. That's Just Not True, April 30, 2024.

picture of a person's daily life. Various technologies can be used to track people's whereabouts, like CCTV and facial recognition cameras, cell-site simulators (Stingrays or IMSI catchers),[66] and automated-license plate readers (ALPRs). ALPR systems collect and store location information about drivers, including dates, times, and locations. This sensitive information can reveal where individuals work, live, associate, worship, or seek reproductive health services and other medical care.[67]

34. One particularly problematic manifestation of geolocation tracking is reverse location searches. According to available information, state use of reverse location searches has been documented in Chile and the U.S. in connection with public protests. Such requests, often backed by a judicial order, invert the logic of investigating specific suspects based on evidentiary grounds justifying the restriction of privacy rights. Rather, reverse searches start from a massive pool of all people's data linked to certain geographical areas, during a particular period, to establish a set of possible suspects. By combining location data and unique device identifiers, authorities could have the capacity to infer everyone present at a specific location and time.

35. Reverse location searches can include the private information of millions of people unconnected to a crime and subject them to further screening with no reasonable justification. They can expose sensitive information, chilling freedoms of expression and association and endangering privacy and other human rights. For example, it has been reported that Chilean prosecutors asked telecom companies to turn over all mobile phone numbers that had connected to cell towers near five of Santiago's subway stations, where fires marked the beginning of the country's 2019 social uprising and protests.[68] According to public information, law enforcement authorities in the U.S. have also used geofence warrants for investigating 2020-2021 Black Lives Matter demonstrations.[69] In addition to issues of legality (such as whether domestic law clearly authorizes this type of search) and suitability (as this technique may skew the investigation, reverse the burden of proof, and lead to abusive use), reverse searches conflict with necessary and proportionate standards.

36. Another geolocation tracking technique relies on exploiting signaling system n. 7 (SS7), the set of telecommunication protocols used to route communications and exchange information between 2G and 3G networks; SS7 is notoriously vulnerable as it lacks robust security protocols.[70] According to information received, between 2019 and 2021, the Brazilian Intelligence Agency (ABIN) reportedly operated a location tracking software known as First Mile, a commercial product designed for SS7 exploitation, to create an undisclosed surveillance system for "parallel" monitoring of the location of individuals considered "enemies" of the government, including journalists, activists, politicians, lawyers, members of the judiciary, and even Supreme Court ministers.[71] On the basis of an inputted phone number, such software could provide the location of a device – and therefore the individual on whose person the device is located – according to its

[66] EFF, Street Level Surveillance, Cell-site simulators/ imsi catchers.

[67] EFF, Dozens of Rogue California Police Agencies Still Sharing Driver Locations with Anti-Abortion States, January 31, 2024; EFF, Street Level Surveillance, Automated license plate readers; 404 Media, License Plate Reader Company Flock Is Building a Massive People Lookup Tool, Leak Shows, May 14, 2025.

[68] La Tercera, Fiscalía pide levantar información de antenas de celulares en días que ocurrieron ataques al Metro, January 6, 2020.

[69] CNET, Geofence warrants: How police can use protesters' phones against them, June 16, 2020; Tech Crunch, Minneapolis police tapped Google to identify George Floyd protesters, February 6, 2021; The Verge, FBI used geofence warrant in Seattle after BLM protest attack, new documents show, February 5, 2022.

[70] Information submitted by Electronic Frontier Foundation (EFF) in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, September 2024, p. 4.

[71] Information submitted by Association for Progressive Communication (APC) in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, pp. 9-10.

position as it connects with a mobile network. The software is capable of monitoring up to 10,000 mobile phone users.[72]

37. According to public reports, the tracking tool was reportedly purchased under a bidding exemption, allowing it to remain secret. This geolocation tracking was deployed later and operated outside of existing legal frameworks.[73] After the Brazilian press revealed the existence of the program, investigations of the ABIN program were undertaken by both the Federal Prosecutor's Office and the Brazilian Federal Police. Investigations indicated that the intelligence agency targeted approximately 2,000 people with the tool, including journalists, activists, politicians, lawyers, and members of the judiciary, as well as people associated with criminal investigations.[74]

38. In 2023, ABIN confirmed that the geolocation system was acquired by the agency in December 2018. According to their statement, the surveillance program was terminated on May 8, 2021, and the agency confirmed it no longer uses the software.[75] According to Federal Police findings, more than 60,000 illegal searches were conducted through First Mile between 2019 and 2021, with at least 12 journalists among the documented targets.[76] On June 12, 2025, the Federal Police submitted the final investigation report to the Supreme Federal Court, and on June 18, 2025, the Court ordered the unsealing of the case records. The investigative phase has been completed, and the case is now in the judicial phase before Brazil's Supreme Federal Court, awaiting prosecution decisions from the Attorney General's Office.[77]

39. In Mexico, according to information received by this Office, SS7-based geolocation tools from various commercial providers have reportedly been purchased and used, including tools that can provide the real-time geolocation of a mobile device based on phone or IMSI number, as well as geofencing.[78] An investigative report revealed that the phone of a journalist Román was geolocated one day before his murder in Chilpancingo, Guerrero, in 2022.[79]

40. Research indicates that other countries in the region would have also utilized the SS7-based surveillance technology provided by Circles – a company affiliated with NSO Group – to engage in tracking and monitoring.[80]

5. Network monitoring, advertising intelligence (AdInt), data brokers, and AI governance frameworks

[72] Information submitted by Electronic Frontier Foundation (EFF) in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, September 2024, p. 4.
[73] Information submitted by Electronic Frontier Foundation (EFF) in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, September 2024, p. 4.
[74] Information submitted by Association for Progressive Communication (APC) in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, pp. 10-11; Information submitted by Electronic Frontier Foundation (EFF) in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, September 2024, pp. 3-8.
[75] Government of Brazil, Brazilian Intelligence Agency (ABIN), Apuração sobre uso de ferramenta de geolocalização, October 20, 2023; CNN Brasil, Entenda o que é o FirstMile, sistema que, segundo a PF, foi usado pela Abin para espionagem ilegal, October 20, 2023.
[76] LatAm Journalism Review, Brazil's intelligence agency spied on reporters to discredit them, police say, July 16, 2025.
[77] Supremo Tribunal Federal, STF retira sigilo de investigação sobre uso de programa secreto pela Abin, June 18, 2025.
[78] Information submitted by R3D in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p.4, 6-7; Information submitted by Article 19 Office for Mexico and Central America in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 6-7.
[79] Information submitted by R3D in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 4; Haaretz, How a Secretive Swiss Dealer Is Enabling Israeli Spy Firms, May 14, 2023.
[80] The Citizen Lab, Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles, December 1, 2020.

41. According to information provided by civil society organizations, during the period from 2019 to 2021, the Brazilian Intelligence Agency has reportedly purchased and used monitoring tools that provide capabilities for mass monitoring of global network traffic and other data, including browsing history and email data.[81] Such tools were allegedly used to surveil politicians, journalists, and ministers of the Supreme Federal Court.[82] Similar monitoring tools were also reportedly purchased by other governments entities in the region.[83]

42. In Mexico, investigative reports indicate that the Attorney General's Office allegedly acquired the mass surveillance platform which can reportedly access location data collected through mobile advertising platforms.[84]

43. Experts on digital technology, security, and human rights note that advertising intelligence (AdInt) is increasingly utilized in surveillance and will continue to play a role into the future, in effect simplifying surveillance options for states. As one academic researcher observed, "It's incredible how much you can get from the exhaust of surveillance capitalism without having to get into someone's phone."[85] Additionally, a number of companies have released marketing brochures that advertise a *combination* of spyware injection and AdInt data, allowing calibration of the malware based on that data.[86] In the age of surveillance capitalism,[87] there exists a marriage of interests between the private sector and states over the expansive collection and analysis of personal data: the same datasets can be deployed for marketing and other profit-making endeavors as well as for state surveillance.

44. The role of data brokers deserves special attention in the digital surveillance ecosystem. Intricate and pervasive private surveillance infrastructure[88] exposes people's daily interaction with various digital technologies. This generates a wealth of data, including location information, that data brokers harvest and then sell to interested buyers. For example, according to reports, U.S. police and intelligence authorities have allegedly used this approach to access people's location data bypassing traditional legal procedures and related due process and privacy safeguards.[89]

45. In 2024, the U.S. Federal Trade Commission (FTC) took action against two data brokers for selling sensitive location data from users.[90] The data was reportedly used to track people in sensitive sites, such as health clinics, places of worship, and military bases. According to the FTC, one of the companies collected over 17 billion location signals from approximately a billion mobile devices daily. It has reportedly sold access to that data to federal law enforcement agencies such as the

[81] Information submitted by Association for Progressive Communications (APC) in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, pp. 11-12; The Brazilian Intelligence Agency confirmed that the geolocation system was acquired in December 2018 and ceased to be used in May 2021. *See* Government of Brazil, Brazilian Intelligence Agency (ABIN), Apuração sobre uso de ferramenta de geolocalização, October 20, 2023

[82] Information submitted by Association for Progressive Communications (APC) in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 12.

[83] Vice, Revealed: US Military Bought Mass Monitoring Tool That Includes Internet Browsing, Email Data, September 21, 2022.

[84] Information submitted by R3D in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 7.

[85] Interview with an academic researcher in personal capacity, August 1, 2024.

[86] Interview with an academic researcher in personal capacity, August 1, 2024.

[87] The Guardian, The goal is to automate us': welcome to the age of surveillance capitalism, January 20, 2019.

[88] EFF, Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance, December 2, 2019.

[89] EFF, Inside Fog Data Science, the Secretive Company Selling Mass Surveillance to Local Police, August 31, 2022; Data Broker Helps Police See Everywhere You've Been with the Click of a Mouse: EFF Investigation, September 1, 2022; NBC, U.S. government buys data on Americans with little oversight, report finds, June 13, 2023.

[90] U.S. Federal Trade Commission, FTC Takes Action Against Mobilewalla for Collecting and Selling Sensitive Location Data, December 3, 2024; FTC Takes Action Against Gravy Analytics, Venntel for Unlawfully Selling Location Data Tracking Consumers to Sensitive Sites, December 3, 2024.

Department of Homeland Security (DHS), the Drug Enforcement Agency (DEA), and the Federal Bureau of Investigation (FBI).[91] An American Civil Liberties Union report has also highlighted that DHS spent significant amounts since 2017 to purchase, without warrants, cell phone location data to monitor movements of both U.S. citizens and foreigners inside the country, at U.S. borders and abroad.[92]

46. In January 2025, the United States adopted Executive Order "Removing Barriers to American Leadership in Artificial Intelligence," which revoked the 2023 Executive Order on the "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence." While the 2023 Executive Order highlighted privacy and civil liberties as guiding principles in AI-related policy and practice, and enumerated steps aimed at mitigation of privacy risks,[93] the 2025 Executive Order does not include reference to privacy or other human rights. Rather, this measure emphasizes promoting U.S. global leadership in AI by removing policies deemed to constrain innovation, and developing AI systems "free from ideological bias or engineered social agendas."[94] While framed as a strategy to foster competitiveness and national security, this shift raises questions regarding the continuity of prior safeguards intended to ensure transparency, accountability, and protection against discriminatory or harmful uses of artificial intelligence in surveillance practices.

47. The U.S. has continued to adjust federal practice and position on AI. According to public information, in April 2025, in line with the new Executive Order, the White House issued two revised policy memoranda on artificial intelligence: *Driving Efficient Acquisition of Artificial Intelligence*[95] and *Accelerating Federal Use of AI through Innovation, Governance, and Public Trust*[96]. These documents, developed in coordination with the Office of Science and Technology Policy, direct federal agencies to expand AI adoption and align governance frameworks with the administration's stated goal of sustaining U.S. global leadership in AI. The first memorandum, which addresses federal acquisition of AI, requires federal agencies to establish policies and processes that "ensure compliance with privacy requirements in law and policy," and manage risks to privacy, civil liberties, and civil rights throughout the "AI acquisition lifecycle."[97] The second memorandum, which directs federal agencies to accelerate the use of AI, requires they maintain "strong safeguards for civil rights, civil liberties, and privacy," including by conducting assessments of the potential impacts of AI in these areas.[98] The memoranda exclude from their scope agencies within the intelligence community.

48. In July 2025, the White House released *Winning the AI Race: America's AI Action Plan*, in compliance with the January Executive Order on "Removing Barriers to American Leadership in Artificial Intelligence."[99] The Action Plan outlines over 90 federal policy measures structured around three pillars: accelerating innovation, building national AI infrastructure, and leading in

[91] Wired, FTC Says Data Brokers Unlawfully Tracked Protesters and US Military Personnel, December 3, 2024.
[92] American Civil Liberties Union (ACLU), New Records Detail DHS Purchase and Use of Vast Quantities of Cell Phone Location Data, July 18, 2022.
[93] Executive Office of the President, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, Executive Order 14110, October 30, 2023, at sections 2(f) and 9.
[94] The White House, Removing Barriers to American Leadership in Artificial Intelligence, Presidential Actions, January 23, 2025.
[95] Executive Office of the President, Office of Management and Budget (OMB), M-25-22: Driving Efficient Acquisition of Artificial Intelligence in Government, April 3, 2025.
[96] Executive Office of the President, Office of Management and Budget (OMB), M-25-21: Accelerating Federal Use of Artificial Intelligence through Innovation, Governance, and Public Trust, April 3, 2025.
[97] Executive Office of the President, Office of Management and Budget (OMB), M-25-22: Driving Efficient Acquisition of Artificial Intelligence in Government, April 3, 2025, at sections 3(d) and 4.
[98] Executive Office of the President, Office of Management and Budget (OMB), M-25-21: Accelerating Federal Use of Artificial Intelligence through Innovation, Governance, and Public Trust, April 3, 2025.
[99] The White House, White House Unveils America's AI Action Plan, July 23, 2025.

international diplomacy and security. Among other elements, the plan emphasizes deregulation, and foresees expanding AI exports, expediting permits for data centers and semiconductor facilities, revising federal regulations deemed to hinder AI development, and establishing procurement guidelines requiring that government contracts with large language model developers ensure systems are "objective" and free from ideological bias.[100] While the plan notes that AI systems should "be built from the ground up with freedom of speech and expression in mind," it includes as a recommendation that the National Institute of Standards and Technology revise its AI Risk Management Framework to "eliminate references to misinformation, Diversity, Equity, and Inclusion, and climate change."[101]

6. Migration-related surveillance

49. Migration-related surveillance is an enormous part of the picture of the development and use of surveillance technologies in the Americas. In a 2021 report, the UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance explored the growing reliance on digital technologies – including biometrics, facial recognition, and other means of surveillance – in the border and immigration enforcement context, a process accelerated by the COVID-19 pandemic.[102] The report indicated that states and non-state actors have used such technologies "in ways that are uniquely experimental and dangerous,"[103] and that use of the technologies has resulted in discriminatory impacts.[104]

50. As Access Now has highlighted, migrants are vulnerable to some of the most serious human rights impacts of surveillance technologies.[105] According to reports, States have sought to enforce border externalization – that is, "the extraterritorialization of national and regional borders to other geographic regions in order to prevent migrant and refugee arrivals"[106] – through the use of "smart borders," leveraging a mix of advanced technologies to predict and control migrants' movements. At the same time, migrants have few if any means to challenge such practices. At the U.S.-Mexico border, migrants have in some cases opted to utilize more dangerous routes for the purpose of avoiding known border surveillance measures, resulting in migrant deaths.[107]

51. The information collected by this Office suggests that the U.S. has relied on surveillance technologies to address migration.[108] The UN Special Rapporteur on contemporary forms of racism detailed in 2021 how U.S. authorities have reportedly incorporated an array of digital tools and

[100] Executive Office of the President of the United States, Winning the Race: America's AI Action Plan, July 2025.
[101] Executive Office of the President of the United States, Winning the Race: America's AI Action Plan, July 2025, p. 4.
[102] UN, Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, E. Tendayi Achiume, Racial and xenophobic discrimination and the use of digital technologies in border and immigration enforcement, A/HRC/48/76, December 17, 2021.
[103] UN, Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, E. Tendayi Achiume, Racial and xenophobic discrimination and the use of digital technologies in border and immigration enforcement, A/HRC/48/76, December 17, 2021, para. 5.
[104] UN, Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, E. Tendayi Achiume, Racial and xenophobic discrimination and the use of digital technologies in border and immigration enforcement, A/HRC/48/76, December 17, 2021, section III.
[105] Access Now, #Migrarsinvigilancia.
[106] UN, Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, E. Tendayi Achiume, Racial and xenophobic discrimination and the use of digital technologies in border and immigration enforcement, A/HRC/48/76, December 17, 2021, para. 49.
[107] Information submitted by Access Now in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 12; interview with Access Now, 20 August 2024; Access Now, "Smart borders" and the making of a humanitarian crisis, March 13, 2023; see also UN, Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, E. Tendayi Achiume, Racial and xenophobic discrimination and the use of digital technologies in border and immigration enforcement, A/HRC/48/76, December 17, 2021, paras 15, 54.
[108] See, e.g., EFF, Border Surveillance Technology.

surveillance technologies – including biometrics, artificial intelligence, and social media screening in addition to surveillance towers and drones – in their treatment of migrants and asylum seekers, which have exacerbated racial and ethnic inequalities and undermined freedom of expression and the right to privacy.[109] The U.S. and Mexico have continued to build out the extensive surveillance apparatus at their border to reduce passage of migrants into U.S. territory. For example, surveillance infrastructure constructed in the Mexican state of Chihuahua reportedly includes "at least 10,000 cameras, 2,000 license plate recognition equipment by video analytics and 11 biometric and facial recognition filters," and is capable of behavior monitoring and prediction.[110]

52. The private sector has responded to the ever-increasing demand for migration-related surveillance technologies, with hundreds of technology companies participating in the U.S. homeland security and surveillance industry.[111] Notably, according to publicly available information, commercial spyware providers have contracted with U.S. Immigration and Customs Enforcement (ICE).[112] Additionally, civil society organizations have expressed concern over multiple contracts entered into between ICE and Palantir Technologies.[113] According to public information, in April 2025, ICE awarded a $30 million contract to Palantir Technologies to develop "ImmigrationOS,"[114] a surveillance platform intended to provide the agency with near real-time visibility over immigration activities, as well as to prioritize enforcement actions against specific groups, including visa overstays. It has been noted that the system consolidates diverse datasets and analytics capabilities, substantially expanding ICE's surveillance capacities.[115]

53. It is noteworthy that migration-related surveillance in the Americas increasingly relies on collection of biometric data. The IACHR previously expressed concern regarding collection of biometric data from migrants, given the risks as such collection presents to privacy and the use of personal data.[116] As enumerated in the *Inter-American Principles on the Human Rights of All Migrants, Refugees, Stateless Persons and Victims of Human Trafficking*, States must provide guarantees for protection of personal data gathered from migrants, including ensuring "the privacy and safe custody of personal data and information."[117] The report of the UN Special Rapporteur on contemporary forms of racism likewise highlighted the human rights risks associated with expansive collection of biometric and other data on migrants and refugees by states and the private sector, which data may subsequently be shared or repurposed. As the UN Special Rapporteur stated, "Data collection is not an apolitical exercise, especially when powerful entities in the global

[109] UN, Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, E. Tendayi Achiume, Racial and xenophobic discrimination and the use of digital technologies in border and immigration enforcement, A/HRC/48/76, December 17, 2021, paras. 54-60

[110] Information submitted by Article 19 Office for Mexico and Central America in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 7; see also EFF, The State of Chihuahua Is Building a 20-Story Tower in Ciudad Juarez to Surveil 13 Cities–and Texas Will Also Be Watching, October 3, 2023.

[111] EFF, Hundreds of Tech Companies Want to Cash In on Homeland Security Funding. Here's Who They Are and What They're Selling, July 8, 2024.

[112] Wired, ICE Signs $2 Million Contract With Spyware Maker Paragon Solutions, October 1, 2024; Electronic Privacy Information Center, Coalition Letter to DHS re: Paragon Solutions, Inc. Contract, October 31, 2024.

[113] Amnesty International USA, Palantir Technologies Contracts Raise Human Rights Concerns before NYSE Direct Listing, September 28, 2020.

[114] Business Insider, ICE just ordered $30 million worth of new technology from Palantir to track immigrants, April 17, 2025.

[115] Wired, ICE Is Paying Palantir $30 Million to Build 'ImmigrationOS' Surveillance Platform, April 18, 2025; The Guardian, Palantir's tools pose an invisible danger we are just beginning to comprehend, August 24, 2025.

[116] IACHR, IACHR expresses concern over migrant DNA collection and policies restricting the mobility of migrant persons in the United States, Press Release No. 279/19, November 1, 2019.

[117] IACHR, Inter-American Principles on the Human Rights of All Migrants, Refugees, Stateless Persons and Victims of Human Trafficking, Resolution 04/19, December 7, 2019, Principle 64.

North collect information on vulnerable populations without being subject to regulated methods of oversight and accountability."[118]

54. These human rights risks are evident in the collection, use, and sharing of migrant data, which have raised privacy and discrimination concerns. For example, the U.S. "Circumvention of Lawful Pathways Final Rule," commonly referred to as the Asylum Ban, required individuals to utilize a mobile application to obtain an appointment to request asylum in the U.S.; without such appointment, asylum seekers were presumed ineligible (unless qualifying for particular exceptions).[119] As Amnesty International detailed, users of the app were required to provide facial photographs and videos of themselves within the app, which U.S. agencies allegedly processed through one-to-many (1:n) facial recognition technology for identity verification and vetting purposes.[120] The app also transmitted geolocation details and unique identifiers of the device.[121] Based on available information, the use of this app as a means of seeking asylum was then eliminated, and the legal status of those migrants who entered the U.S. through use of the app was revoked,[122] though it is unclear what will become of the data already collected. In 2025 the Department of Homeland Security released a new version of the application to facilitate a process of "self-deportation."[123] The new application reportedly relies on the same technical architecture and poses the same privacy and security issues, as it continues to collect facial biometric data and geolocation details.[124] Ultimately, migrants have had little choice but to provide such data in order to access critical services, putting them at increased risk of discriminatory impacts and privacy violations. According to public information, ICE is indeed utilizing a mobile phone app that relies on such biometric data for migrant identification.[125]

55. Moreover, human rights risks are compounded when biometric data is shared between agencies or among States without appropriate safeguards. For example, in January 2025 the U.S. Department of Justice directed a number of federal agencies under its authority[126] to disclose to the U.S. Department of Homeland Security all "identifying information and/or biometric data relating to non-citizens located illegally in the United States" that they possessed in their files, for the purpose of "facilitating appropriate removals, enforcement actions, and immigration-related investigations and prosecutions,"[127] regardless of the original basis for the agencies' collection and use of the data. According to investigative reporting, the U.S. government is relying on Palantir Technologies' data integration and analytics tools for the purpose of merging and analyzing data across multiple agencies.[128]

56. Recent reports also indicate that, under the 2025 U.S. administration, migration-related surveillance has expanded through broader inter-agency initiatives. In particular, the Department of Government Efficiency (DOGE) has reportedly promoted the consolidation of multiple federal databases —including records from the Department of Homeland Security, the Social Security

[118] UN, Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, E. Tendayi Achiume, Racial and xenophobic discrimination and the use of digital technologies in border and immigration enforcement, A/HRC/48/76, December 17, 2021, para. 12.
[119] Amnesty International, USA: CBP One: A blessing or a trap?, May 8, 2024, p. 12-15.
[120] Amnesty International, USA: CBP One: A blessing or a trap?, May 8, 2024, p. 45-47.
[121] Amnesty International, USA: CBP One: A blessing or a trap?, May 8, 2024, p. 46.
[122] PBS News, Homeland Security revokes legal status for migrants who entered U.S. using CBP One app, April 8, 2025.
[123] Biometric Update, DHS replaces CBP One app with CBP Home; Amends regs for alien fingerprinting, March 11, 2025.
[124] Biometric Update, DHS replaces CBP One app with CBP Home; Amends regs for alien fingerprinting, March 11, 2025.
[125] 404 Media, ICE Is Using a New Facial Recognition App to Identify People, Leaked Emails Show, June 26, 2025.
[126] FBI, DEA, ATF, U.S. Marshals Service, Federal Bureau of Prisons.
[127] U.S. Department of Justice, Interim Policy Changes Regarding Charging, Sentencing, And Immigration Enforcement, January 21, 2025.
[128] The New York Times, Trump Taps Palantir to Compile Data on Americans, May 30, 2025.

Administration, and the Internal Revenue Service—into a centralized repository concerning migrants.[129] These measures have been framed as efforts to eliminate information silos across agencies, but civil society and media reports have noted that they could significantly increase the scale of inter-agency data sharing and surveillance capacities.[130] Public reports have further highlighted that artificial intelligence tools are being deployed in this process, raising additional questions regarding data protection and privacy safeguards.[131] In April 2025, the Department of Homeland Security, together with USCIS and DOGE, announced a comprehensive overhaul of the Systematic Alien Verification for Entitlements (SAVE) database, aiming to provide a single nationwide platform for verifying non-citizen status by integrating criminal records, immigration histories, and addresses, while eliminating search fees and expanding access to multiple government levels.[132]

57. Civil society organizations have highlighted the human rights implications of DOGE's access to federal administrative databases. According to a joint analysis by the Center for Democracy & Technology and The Leadership Conference's Center on Civil Rights and Technology, DOGE has reportedly obtained access to sensitive records from multiple federal agencies, including information on refugees, asylum seekers, and even migrant children. The report warns that repurposing such administrative data for immigration enforcement purposes could lead to wrongful deportations, denial of access to essential social services, and increased risks of misidentification, data breaches, and discriminatory impacts.[133]

58. Practices of cross-border data sharing raise additional concerns. Public information shows that the U.S. has for many years shared migration-related biometric data with other States in the Americas.[134] The Department of Homeland Security acknowledged a number of privacy risks associated with such Biometric Data Sharing Partnerships, including the possibility of non-compliance with the principles of purpose specification, data minimization, and use limitation.[135] Yet this Office observes that sharing of migrants' biometric data is on track to expand: in March 2025, the U.S. and Colombia signed a letter of intent on biometric data sharing, with the U.S. committing "to assist Colombia in deploying biometric technologies to enhance the identification and tracking of individuals crossing borders."[136] Additionally, the U.S. and Mexico entered into a statement of cooperation on biometric immigration information sharing in 2017.[137]

59. The myriad of techniques utilized in surveillance, and the cross-referencing, sharing, and utilization of data obtained through various surveillance technologies, highlight the need for holistic reforms that address diverse tactics and state policy cohesively, and are adaptable to

[129] Wired, DOGE Is Building a Master Database to Surveil and Track Immigrants, April 18, 2025.
[130] The Conversation, From help to harm: How the government is quietly repurposing everyone's data for surveillance, April 23, 2025.
[131] Tech Policy Press, DOGE Is Using AI to Centralize Government Power. It's Time to Flip the Script, May 2, 2025.
[132] U.S. Department of Homeland Security (DHS), DHS, USCIS, DOGE Overhaul Systematic Alien Verification for Entitlements Database, Press Release, April 22, 2025.
[133] Center for Democracy & Technology (CDT) and The Leadership Conference's Center on Civil Rights and Technology, Immigration, DOGE, and Data Privacy, May 9, 2025.
[134] Center for Strategic and International Studies, Tracked: Stories at the Intersection of Migration, Technology, and Human Rights, December 15, 2022; U.S. Department of Homeland Security, Fact Sheet: DHS Agreements with Guatemala, Honduras, and El Salvador.
[135] U.S. Department of Homeland Security, Privacy Impact Assessment for the DHS International Biometric Information Sharing Program (IBIS) - Biometric Data Sharing Partnerships (BDSP), November 18, 2022; Access Now, Joint statement: Mexico, Guatemala, Honduras, El Salvador and the United States must terminate their agreements on cross-border transfers of migrants' biometric data, March 23, 2023.
[136] Biometric Update, United States and Colombia deepen security ties with biometric data-sharing pact, March 31, 2025.
[137] Statement of Cooperation Between the Secretariat of Governance of the United Mexican States, National Migration Institute and the Department of Homeland Security for the United States of America Concerning Biometric Immigration Information Sharing.

technological changes over time. As Access Now has described, "Surveillance is an apparatus, a mixture of the technologies;"[138] it draws on a wealth of information from digital profiling, ICT providers, social networks, and other sources, as well as facial recognition, spyware attacks, and other intrusive measures. "This is one of the most critical parts of surveillance in Latin America as a whole. It's not only technologies, it's the use of tactics, techniques that are working together."[139]

B. Normalization of surveillance

60. These ever-expanding manifestations of surveillance also reflect how deeply embedded in society surveillance has become, with the end result that intrusive surveillance practices and surveillance technologies are increasingly normalized. Academic researchers and experts describe surveillance as being "on the radar of the public. It's a topic well-covered in the media and brought to the attention of policy makers." At the same time, surveillance technology "has become an industry that has normalized. It is taken for granted that this goes on. It's a bit of a contagion effect when people hear about it. Government operators now see this as something legitimate to use. What was once quite shocking is now seen as normal."[140]

61. In the Americas, NGOs have noted that the normalization of "high-end" technological surveillance may have been facilitated by the normalization of "low-end" surveillance practices prevalent in the past, such as telephone tapping and physical surveillance.[141] The Electronic Frontier Foundation (EFF) assessed that a cultural shift is required:

> In Latin America, we have a long-standing culture of secrecy regarding surveillance—a legacy of military dictatorships with a particular approach to security. Such opacity is even worse with intelligence agencies, under the belief that public oversight about their activities would undermine the government's ability to counter national security threats. This mindset permeates not only law enforcement but also public opinion. After all, there's the belief that part of doing security well is not disclosing how things are done. … Yet when abuses occur, rights are violated at scale. That isn't security; it's the opposite. It harms people rather than tackling real threats to the country.[142]

62. Access Now similarly noted that politicians in the Americas frequently present "the benefits of facial recognition in a techno-solutionist way, pitching that the problems will be solved immediately with cameras. They use rhetoric about 'nothing to hide.' This is a populist measure, because it is presented as the solution for criminality. In general, facial recognition is seen with positive eyes in Latin America," though public sentiment in Brazil has proven an exception due to the efforts of civil society there.[143]

63. A human rights defender whose device was infected with Pegasus, reflected:

> On the one hand, in Mexico the issue of telephone tapping against everyone is very normalized. I think this is sometimes repeated in the logic of "Mexico is not in the

[138] Interview with Access Now, August 20, 2024.
[139] Interview with Access Now, August 20, 2024.
[140] Interview with an academic researcher in personal capacity, August 1, 2024.
[141] Interview with SocialTIC, August 19, 2024.
[142] Interview with Electronic Frontier Foundation (EFF), August 19, 2024.
[143] Interview with Access Now, August 20, 2024.

worst situation of how El Salvador is", or other parts of the world where this technology is used.[144]

64. The Special Rapporteur assesses that it is no coincidence that the normalization of the surveillance practices highlighted herein has taken place against a backdrop of government digitization, widespread adoption of digital identity systems,[145] and expansive state use of direct access.[146] Many states have incorporated or are developing digital identity systems, which use centralized registries including biometric data, and which raise concerns about integration of digital ID systems into broader surveillance infrastructures.[147] In the absence of robust human rights safeguards, these trends may ultimately push states toward an all-out embrace of mass surveillance.

65. The normalization of surveillance practices has been significantly accelerated by regional digitalization initiatives that, while presented as modernization efforts, create expansive surveillance infrastructures. The 2026 Digital Agenda for Latin America and the Caribbean (eLAC 2026), approved in November 2024 during the Ninth Ministerial Conference on the Information Society in Latin America and the Caribbean, explicitly promotes the "digital transformation of the State" and the improvement of digital identity systems to facilitate access to public services and promote cross-border digital services within a framework of regional integration[148].

66. As EFF has observed, while digitalization can streamline access to public services, "it can also make them less accessible, less clear, and put people's fundamental rights at risk." While human rights protection should define State metrics for efficiency and success, "efficiency" in practice often manifests as budget cuts and restricted access to public services, undermining core rights.[149]

67. Particularly concerning is that digital identity and data-interoperability systems "are generally treated as a natural part of government digitalization plans," yet they can be expanded into "a potential regime of unprecedented data tracking." The most vulnerable populations—those most in need of effective government interaction—are also those most prone to having scarce access to digital technologies and limited digital skills, making them susceptible to exclusion or enhanced surveillance.

68. The normalization of digital surveillance does not occur in a political vacuum, but frequently coincides with broader processes of democratic erosion in the region. The Special Rapporteur observes with particular concern that the expansive use of surveillance technologies has created conditions conducive to the development of authoritarian tendencies in several States of the Americas.

69. Mass surveillance and targeted surveillance practices documented in this report not only violate individual rights, but erode the essential pillars of democracy: separation of powers, judicial

[144] Testimony No. 26, obtained on October 9, 2024.
[145] Derechos Digitales, Identidad digital en América Latina: situación actual, tendencias y problemáticas, September 2023; EFF, Digital Identification Must Be Designed for Privacy and Equity, August 31, 2020.
[146] Direct access is the retrieval by state authorities of personal data directly from a service provider's infrastructures, without having to make an individualized request to the provider, or even notify them or the user, thus bypassing safeguards required by human rights law. See https://globalnetworkinitiative.org/defining-direct-access/
[147] Information submitted by an independent expert in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, July 2024; Derechos Digitales, Digital Identity in Latin America: Current situation, trends and problems, September 2023.
[148] Electronic Frontier Foundation (EFF), Deepening Government Use of AI and E-Government Transition in Latin America: 2024 in Review, January 1, 2025.
[149] Electronic Frontier Foundation (EFF), Deepening Government Use of AI and E-Government Transition in Latin America: 2024 in Review, January 1, 2025.

independence, freedom of expression and civic space. When States can monitor journalists, human rights defenders, political opponents, and civil society on a widespread basis, the mechanisms of democratic accountability are undermined, creating systems that maintain electoral facades while restricting opposition activities.

70. The emergence of "algorithmic governance" represents a qualitatively new form of surveillance that extends beyond monitoring into automated control. Recent AI strategies in Costa Rica[150] and Brazil[151] envision "personalized services to citizens" and "proactive" government interventions based on algorithmic analysis of citizen data. While presented as efficiency measures, these systems involve "the massive amount of personal data, including sensitive data, that those systems may process and cross-reference," creating what EFF has characterized as "potential biases and disproportionate data processing in risk assessment systems."[152]

71. The Special Rapporteurship also observes with alarm the development of "predictive surveillance" systems. For instance, the recent establishment of the "Unit of Artificial Intelligence Applied to Security" (UIAAS) in Argentina, with powers to "patrol open social networks, applications and Internet sites" and use machine learning algorithms for crime prediction, exemplifies how AI-enhanced surveillance can institutionalize discriminatory targeting while maintaining a veneer of technological objectivity.[153]

72. It also notes that the datafication of governance fundamentally alters the citizen-State relationship. When government services become contingent upon digital identity systems that enable comprehensive tracking, and when AI systems assess individuals' "risk profiles" for accessing services or benefits, citizenship itself is transformed into a surveillance relationship. This represents the ultimate normalization of surveillance: a system where being watched becomes the prerequisite for accessing rights.

73. The Special Rapporteurship observes that the normalization of digital surveillance is a powerful trend, facilitated by government digitization and the monetization of user data online. It is well established that international human rights law considers the use of intrusive surveillance measures by states to be an exceptional activity, that is, falling within carefully circumscribed exceptions. Increasingly, however, states have demonstrated, in rhetoric and practice, that they do not consider intrusive surveillance practices exceptional in the first instance. This inversion of the legal framework—treating surveillance as the norm rather than the exception—represents a fundamental challenge to the rule of law and democratic governance.

C. Human rights impacts of surveillance abuses

74. According to information received by this Office, states have used digital surveillance as a means of control over civil society organizations, human rights defenders, journalists, lawyers, political opposition, and other regime critics or social advocates. Civil society organizations have emphasized that use of surveillance technology is frequently an indicator of a crackdown on the

[150] Costa Rica, Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), Estrategia Nacional de Inteligencia Artificial de Costa Rica 2024-2027, 2024.
[151] Brazil, Ministério da Gestão e Inovação em Serviços Públicos (MGI), Novo Plano Brasileiro de Inteligência Artificial prevê o investimento de R$ 1,76 bi para melhoria de serviços públicos, July 30, 2024.
[152] Electronic Frontier Foundation (EFF), Deepening Government Use of AI and E-Government Transition in Latin America: 2024 in Review, January 1, 2025.
[153] República Argentina, Boletín Oficial, Resolución 710/2024, July 26 2024.

civic space, impacting freedom of expression, freedom of association, and other rights.[154] When discontent increases among populations, people become more vocal in challenging power, while at the same time there is less tolerance from those in power to be criticized.[155] Surveillance tools are used to maintain control[156] and preserve power.[157]

75. It is important to acknowledge as well that, within states in the region[158] where organized criminal groups maintain a strong presence – creating systems of "parallel power" – there is a risk of collusion between state authorities and organized crime in the use of surveillance. [159] Such collusion creates the potential for deployment of surveillance technologies *for the benefit of* organized crime, thus compounding the risks to security and human rights associated with those technologies.

76. The use of digital surveillance technologies poses an existential threat to the right to privacy, which threat is made more acute by a climate of state digitization and normalization of surveillance. The right to privacy, enshrined in Article 11 of the American Convention on Human Rights and Article 17 of the International Covenant on Civil and Political Rights, serves as a foundational right that enables the exercise of numerous other human rights. As the Inter-American Court of Human Rights has established, privacy encompasses not only the protection of personal data and communications, but also the broader concept of "informational self-determination"—the right of individuals to control how their personal information is collected, processed, and used.

77. In the context of digital surveillance, privacy violations are particularly severe because modern technologies enable the collection and analysis of vast amounts of intimate information about individuals' daily lives, relationships, beliefs, and activities. Digital surveillance can be continuous, comprehensive, and retrospective, creating detailed profiles of individuals that reveal the most intimate aspects of their lives. The Inter-American system's recognition of privacy as encompassing both negative obligations (the duty to refrain from arbitrary interference) and positive obligations (the duty to protect privacy from third-party violations) is especially relevant in the context of commercial surveillance technologies.

78. The Special Rapporteur notes that digital surveillance violations of privacy are particularly insidious because they often remain invisible to the affected individual, creating a state where the violation of rights occurs systematically but remains hidden from both the victim and the broader public. Numerous manifestations of harm flow from impingement on that foundational right.

79. The human rights impacts of surveillance are serious and wide-ranging, and it is essential for the discourse around surveillance reform to center those impacts. In the Americas, four key trends stand out: societal-level chilling effects on freedom of expression, freedom of movement, and other rights as a result of the normalization of surveillance and surveillance abuses; the use of surveillance to undermine investigative and critical journalism and human rights defense; the intersectional and gender-based harms resulting from surveillance; and the impunity associated with digital surveillance abuses, which results in a state of continuous harm against, and ongoing violation of the rights of, targeted individuals.

---

[154] Interview with Amnesty International's Security Lab, August 8, 2024.
[155] Interview with Amnesty International's Security Lab, August 8, 2024.
[156] Interview with Amnesty International's Security Lab, August 8, 2024.
[157] "Surveillance is a tool not to combat crime or terrorism but a tool to preserve power. Not only institutional power, but the power that governs societies; not just state power, but a network of power that involves organized crime, the state, business people. Surveillance is a key factor in repression and corruption." (Interview with R3D, August 23, 2024).
[158] Interview with R3D, August 23, 2024; Information submitted by Association for Progressive Communications (APC) in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 19.
[159] Americas Quarterly, Latin American Organized Crime's Real Target: Local Government, February 18, 2025.

80. In preparing this report, the Special Rapporteurship collected testimonies from individuals in the Americas who were subjected to surveillance through infection of their mobile devices with Pegasus spyware, as confirmed by independent investigations of civil society groups and journalists. Many of these individuals described chilling effects on their expression, work, and other activities, as well as ongoing psychological harm. Many also noted that the intrusive surveillance was one element, alongside online harassment and disinformation campaigns, of what researchers have described as a hostile digital environment for civil society, journalists, and transnational activism at large.[160] Their testimonies are included throughout this discussion.

1. Surveillance generates widespread chilling effects on freedoms of expression, peaceful assembly, association, movement and thought

81. As more and more individuals are targeted with invasive surveillance technologies in violation of their internationally-recognized human rights, "there is a change in recognition of how widespread the use can be, and in the common imagination of who can be put under surveillance. You start to see peers experiencing it, and start to realize that I too can be put under surveillance."[161]

82. Amnesty International has described the normalization of surveillance as an "indicator of a chilling effect that hinders journalists, HRDs [human rights defenders] and anyone else in the civic space from fully exercising their human rights."[162] Normalization of surveillance is observed to have two key outcomes with respect to the expression and activities of human rights defenders, journalists, and other members of civil society. On the one hand, people may become inured to the notion that they are surveilled, choosing to compartmentalize and focus their limited resources on the work in which they are engaged, accepting surveillance as an unavoidable risk attached to that work.[163] NGOs have noted, however, that such acceptance can create challenges to raising awareness of the impact of surveillance technologies and methods to effectively enhance digital security.[164] On the other hand, individuals may self-censor or limit their activities in order to prevent exposure to surveillance, harassment, and other repercussions.[165] In both cases, individuals may experience lasting psychological impacts, including intense stress, fear, guilt, and paranoia about technology.[166]

83. An individual whose device was infected with Pegasus spyware in apparent connection with a public commentary on the government's economic policies, reflected that the surveillance caused her to self-censor dramatically. In addition to the spyware infection, she experienced regular harassment campaigns on social media networks. She felt she was being watched digitally and physically, putting herself at risk with her work, and came to the conclusion that self-censorship was the only way to stay safe. She chose to adjust her public commentary as a result. She has also changed her patterns of social behavior and mobile phone usage, and reports feeling a very internalized censorship, operating under the assumption that everything she writes is being read by the government. She has turned down career opportunities that she feels may increase her exposure, and feels her career options are curtailed.[167]

[160] Interview with an academic researcher in personal capacity, August 6, 2024.
[161] Interview with Amnesty International's Security Lab, August 8, 2024.
[162] Information submitted by Amnesty International, Americas Regional Office, in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 4.
[163] Interview with SocialTIC, August 19, 2024; interview with Amnesty International's Security Lab, August 8, 2024.
[164] Interview with SocialTIC, August 19, 2024.
[165] Interview with SocialTIC, August 19, 2024.
[166] Interview with SocialTIC, August 19, 2024; Interview with an academic researcher in personal capacity, August 1, 2024.
[167] Testimony No. 17, obtained on October 29, 2024.

84. Moreover, as explored in section II.A.6, migrants in the region have experienced significant chilling effects as a result of surveillance, which have undermined their ability to safely seek asylum.

85. Lastly, beyond its impact on freedom of expression and association, surveillance can also undermine the right to freedom of thought and conscience. This right protects the internal process of thought formation, which is distinct from, but closely connected to, freedom of opinion and expression.[168] The knowledge or suspicion of being monitored may influence not only what individuals choose to express publicly, but also how they form private convictions, explore ideas, and engage in the development of their personal worldview. In such contexts, individuals may unconsciously alter their mental processes and belief formation to avoid potential scrutiny, resulting in a form of self-censorship. This chilling effect threatens the integrity of the *forum internum*, which is protected under international human rights law and cannot be subject to limitations. No one shall be compelled to reveal their thoughts[169], and States or non-State actors may violate this right when they punish or retaliate against individuals for their thoughts, regardless of whether those thoughts were accurately identified or not.[170]

86. As the United Nations Special Rapporteur on freedom of religion or belief has emphasized, "as technological advances increase the possibility of accurately decoding or inferring one's inner mind, clear parameters and protections for *forum internum* rights need urgent consideration."[171] The protection of freedom of thought "is predicated on the principle that everyone is free to think whatever they wish within their inner mind."[172]

2. *Surveillance undermines human rights defense and investigative and critical journalism*

87. Surveillance is a potent tool in broader adversarial campaigns designed to reinforce state narratives and control, and undermine political opposition. In some cases, surveillance has preceded physical violence.[173] In other cases, surveillance has fueled disinformation campaigns against journalists and human rights defenders, as reflected in interviews conducted by the Special Rapporteurship. Access Now has observed a "combination of repression and surveillance" that creates "immense impact in terms of civil society. If you consider the impact on environmental organizations, accountability organizations, anti-corruption organizations, it is regression in the region . . . breaking apart the tissue of civil society and opposition."[174]

---

[168] UN, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan, Disinformation and freedom of opinion and expression, A/HRC/47/25, April 13, 2021, para. 33; Report of the Special Rapporteur on the promotion and promotion and protection of the freedom of opinion and expression, Research report on artistic freedom of expression, A/HRC/44/49/Add.2, July 24, 2020, para. 11.

[169] UN, Human Rights Committee, General comment adopted by the Human Rights Committee under article 40, paragraph 4, of the International Covenant on Civil and Political Rights, CCPR/C/21/Rev.1/Add.4, September 27, 1993, paras.1,3.

[170] UN, Report of the Special Rapporteur on freedom of religion or belief, The Freedom of Thought, A/ 76/380, October 5, 2021, para 27.

[171] UN, Report of the Special Rapporteur on freedom of religion or belief, The Freedom of Thought, A/ 76/380, October 5, 2021, para 27.

[172] UN, Report of the Special Rapporteur on freedom of religion or belief, The Freedom of Thought, A/ 76/380, October 5, 2021, para 27.

[173] Information submitted by R3D in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 3-4; Haaretz, How a Secretive Swiss Dealer Is Enabling Israeli Spy Firms, May 14, 2023; Forbidden Stories, Pegasus: The new global weapon for silencing journalists, July 18, 2021.

[174] Interview with Access Now, August 20, 2024.

88. For example, a member of the International Group of Independent Experts (GIEI) investigating the disappearances in Mexico noted that the infection of his phone with Pegasus was part of the broader and ongoing campaign to discredit the GIEI. He found that "the accumulation of situations [the smear campaign and the Pegasus infection] was a very hard cocktail to face psychologically. The Pegasus infection was part of a strategy to hinder and not let the work of the GIEI advance."[175]

89. Another human rights defender that was also working on the disappearances in the Ayotzinapa case indicated that audio recordings of conversations held with the parents of the disappeared students had been leaked online, in a context suggesting the work was part of the efforts of an organized criminal group, in order to delegitimize their work.[176]

90. A human rights defender and lawyer described how the state has created an atmosphere of fear and self-censorship, achieved not "in a generalized way, but [through] a surgical stigmatization." Select individuals associated with advocacy work and civil society activities are targeted, including through surveillance, contributing to closure of the civic space. He believes he was infected with Pegasus spyware due to his high-profile human rights defense activities. He described the impact of the experience:

> You feel violated, you feel that someone has entered your house, has been present in family conversations, with friends, with work partners, it is an ugly invitation. When you understand that they can listen to you, take pictures, videos, download information, it gives you a feeling of disgust towards these guys. Where is my information that is intimate, that belongs to my family? You go from anger to anger and to take precautions.[177]

91. A journalist targeted with Pegasus spyware further explained the campaign against El Faro:

> When the current administration arrived in 2019, we saw his first hostile behavior against the press, and his very clear and specific interest in undermining the credibility of our media outlet. Then, I began to feel like a victim of state bullying. I was physically blocked from a press conference of the vice presidency of the republic in September 2019. That level of hostility I had never received before. Then in September of the following year, in a press conference, already with the pandemic and the confinement, I had a verbal exchange with the president. The president was very rash, turned off my microphone, and accused El Faro of money laundering. He was very hostile. I noticed that there was a special effort against El Faro.[178]

92. This journalist noted the correlation in timing between spyware infections and El Faro's coverage of sensitive issues: "I identif[ied] the date of the attacks and what I was working on in the previous days. Many were when I had just published something… From *El Faro* we noticed a very clear coincidence for example in coverage of gang negotiations with Pegasus infections."[179]

[175] Testimony No. 22, obtained on November 11, 2024.
[176] Testimony No. 26, obtained on October 9, 2024
[177] Testimony No. 07, obtained on October 30, 2024.
[178] Testimony No. 04, obtained on October 9, 2024.
[179] Testimony No. 04, obtained on October 9, 2024.

93. All of the individuals interviewed by the Special Rapporteurship believe that state entities subjected them to intrusive surveillance due to their journalism, rights defense work, or "speaking out" about state policies or individuals in power. Access Now reiterates that "spyware is used specifically to persecute journalists and human rights defenders."[180]

94. This extralegal deployment of surveillance technology by a state erodes the ability, and in some cases the will, of journalists and rights defenders to engage in their work. States may use surveillance tools to obtain preemptive knowledge of critical reporting and advocacy, or information regarding sources and political opposition, but the impact of surveillance is not limited to such first-order effects. Without intervention or support to those targeted, surveillance fundamentally alters the expectations and risks associated with such work, threatening to undermine critical journalism and human rights defense at large.

95. The individuals with whom the Special Rapporteurship spoke mentioned that they had experienced significant impacts on their physical and mental health as a result of the use of Pegasus spyware against them. Some expressed great concern for the potential impact of such surveillance on their families or other relationships. Many reflected on the chilling effect of invasive surveillance on their journalism or rights defense work. Some rights defenders and journalists acknowledged that they self-censored following their experiences of surveillance. Others felt that they did not self-censor outright and continued to work on sensitive issues, but noted that their digital interactions had become less frequent, more anxiety-inducing, and more security-focused, with an overall sense that they could not express themselves freely or share information. Many individuals interviewed conveyed a sense of vulnerability, knowing that state actors could access personal or work-related information on their devices at any time.

96. A journalist who had previously received digital security training, related that when she first learned her device was infected with Pegasus spyware:

> It was very shocking: we went from something that was a very distant possibility, to something concrete. . . . I felt, why? I felt very lonely and scared. I didn't know what to do, whether to throw the phone away . . . Even though they told you how to prevent and all that, they didn't prepare you for the emotional impact. Thinking that they had had access to photos, conversations . . . .[181]

97. A human rights defender understood the infection of his device with Pegasus to be a consequence of speaking out and criticizing the government. The surveillance was part of "the construction of a context to delegitimize all those who are critical," to "generate fear in society," and has resulted in significant chilling effects. "There is no longer a person from civil society who feels safe." The surveillance made him feel that "what is yours is no longer private, it is not safe," and he continues to experience stress, though he reported that he has normalized the potential for surveillance in his life. After the Pegasus infection, journalists and others started to avoid him or treat him as an "anticipated political prisoner." He is concerned that his family may be targeted by the state as well, and their forms of communication have changed; he operates under the assumption that "a family photo shared by WhatsApp is a photo shared with the government."[182]

[180] Interview with Access Now, October 2, 2024.
[181] Testimony No. 21, obtained on October 3, 2024.
[182] Testimony No. 13, obtained on October 28, 2024.

98. A lawyer and human rights defender whose device was infected with Pegasus described ongoing feelings of self-censorship, terror, and anger, for which she sought professional therapy. She has experienced panic attacks, had second thoughts about continuing in her rights defense work, and doubted her own abilities. The surveillance affected her personal relationships and sense of security at home, and she has curbed the use and presence of her mobile device, as she no longer trusts it.[183]

99. A journalist reflected that the infection of his device with Pegasus left him with feelings of defenselessness, helplessness, and guilt. He and many of his colleagues had already adopted strict digital and physical security protocols, which did not prevent this surveillance. He felt guilty for failing to protect his sources and for having been infected at all. Overall, however, he felt that "Pegasus is just one more manifestation of what it means to defy the official narrative", one of many risks to journalists.[184]

100. A journalist also stated:

> Learning that my personal phone was attacked was very devastating because of the nature of the information I had on it. All of that information, such as banking information, sensitive information, was indeed put at risk.[185]

101. She warned that investigative journalists are adjusting their routines in light of the digital security threats they face:

> The world of investigative journalists here is very small, and we are all very connected. I have noticed that instead of meeting in open places we prefer to stay more in places where we feel there is more protection, privacy, avoiding any kind of exposure. That can avoid problems such as exposure on social networks.[186]

102. Another journalist who experienced a Pegasus infection also described feeling afraid for herself and her sources. The incident traumatized her and made her feel responsible for taking care of her family, who were also afraid after the Pegasus infection came to light. She considers that the surveillance was in itself a kind of deterrent to the practice of journalism: when the infection happened, she asked herself, "Is that how it is to be a journalist?" While she decided to stay at the media outlet she was working,

> [t]his type of infection only shows what it means to be a journalist (...), where there is a giant apparatus with which you cannot compete, they are gradually drowning journalism. It is hard to see other colleagues and their families threatened, there are no guarantees for the practice of journalism.[187]

103. Another journalist infected with Pegasus stated:

> I have not experienced self-censorship as such, but I have forced myself to be more careful about how I take care of my sources. I continue to work on the same topics I used to work on, and now in terms of documenting human rights violations. I try

[183] Testimony No. 23, obtained on November 1, 2024.
[184] Testimony No. 12, obtained on October 28, 2024.
[185] Testimony No. 08, obtained on October 1, 2024.
[186] Testimony No. 08, obtained on October 1, 2024.
[187] Testimony No. 11, obtained on November 8, 2024.

> to say things on social networks, to express myself in the same way I have always done. But I have lowered my profile, but because of time issues... it consumes me to spend a lot of time in that space that has become very toxic. From one moment to another I feel that the scenario is going to change, it's going to be more inquisitive, and it's going to be more difficult to do the work we are doing now.[188]

104. Another journalist interview by this Office noted that the use of Pegasus was "of very public interest" and "has had very great deterrence with friends. Without being asked, I put my phone away. It is a matter of my self-censorship... It is very difficult for me to reach people because I am not so adventurous. I feel a decrease in the flow of information."[189]

105. From the interviews with Pegasus victims, it is apparent that surveillance creates a dual impact: journalists become more cautious about communication security and data integrity, and experience a deterrent effect on their work, especially on certain sensitive topics. On the other side, sources become increasingly reluctant to engage due to potential surveillance exposure.

106. Many individuals with whom the Special Rapporteurship spoke indicated that surveillance creates barriers between themselves and their sources, thereby undermining access to the critical information on which journalism and rights defense relies. They reported that this deterioration of journalist-source relationships significantly impairs investigative reporting and accountability journalism. Surveillance disincentivizes sources from making contact or sharing information, as they feel it will put them at increased risk for identification and persecution.

107. Some of the individuals interviewed had determined that their spyware infections happened around the same time as publication of reports relying on sensitive government sources, suggesting the purpose of the surveillance may have been source identification. A journalist pointed out that state authorities had already threatened to sue his media outlet if it did not reveal the sources for a sensitive story.[190] His media outlet reported on issues of corruption and improper spending during the pandemic as well. Their sources began to report that they were being asked about their contacts with journalists, and felt afraid to speak to the media. The Pegasus spyware infections of the journalists with that media outlet occurred in this context of source investigation and intimidation. As the journalist explained,

> One of the ways in which Pegasus affected us the most is that several of our sources became very afraid. And that made it almost impossible to continue working with them. They won the battle. They were very afraid of them. In fact, when the report was revealed and when Apple made its own report and revealed that even officials were being spied on, that added more fear. Because even officials are being spied on . . . . Several of those sources to this day are closed.[191]

[188] Testimony No. 08, obtained on October 1, 2024.
[189] Testimony No. 04, obtained on October 9, 2024.
[190] Testimony No. 03, obtained on September 30, 2024.
[191] Testimony No. 03, obtained on September 30, 2024.

108. Another journalist likewise said,

> "I had a suspicion that I was being tapped even before I knew it. I noticed that the sources I was in contact with were being transferred or removed from their position. It really caught my attention."[192]

109. Other testimony received by the Office stated:

> About the sources, I particularly noticed a withdrawal from people I used to interact with on social networks, or on WhatsApp, on messaging channels. I noticed like sources were aware that there was someone watching, and that they had to be more cautious. Extra barriers were created between journalist and source... and that distanced them, or set the tone from that moment on. Certainly now the flow of information that arrives by telephone is much less than it used to be.[193]

110. Moreover, methods of protecting sources have become more onerous, creating further disincentives to engagement. A journalist indicated, "We had occasions when we had to show our sources how to encrypt information, or use more secure email. We showed them how to have encrypted keys and how to decode them. We have sources that are still collaborating with us, but we had to teach them how to have more secure communications."[194]

111. A journalist likewise noted the challenge of enhancing security with sources: "The day to day and the fact of explaining to the sources it's a big challenge ... I have to explain to them that they have to download certain programs... applications...they don't like it. They prefer not to talk, some of them."[195]

112. A journalist commented:

> At that time [of the Pegasus infection] the sources I had, we moved them to another type of more secure communication. Luckily these people were a little bit aware. With other people it was more difficult because teaching them to use [the secure application] ... it was difficult, they used WhatsApp. Personally, before this came out I noticed that the sources themselves were self-censoring. They were public employees. This put an end to it for some, but others even before that were blocking themselves.[196]

113. Individuals have also reported financial impacts and a changed relationship with technology. Their energies and resources have been directed to digital security efforts rather than the work itself. For example, some described upgrading equipment (though such upgrades are constrained by resource availability), switching to US lines, using VPNs and more secure messaging and email platforms, or leaving cell phones behind for sensitive meetings or movement.

[192] Testimony No. 04, obtained on October 9, 2024.
[193] Testimony No. 04, obtained on October 9, 2024.
[194] Testimony No. 03, obtained on September 30, 2024.
[195] Testimony No. 05, obtained on October 9, 2024.
[196] Testimony No. 21, obtained on October 3, 2024.

114. A human rights defender explained that his organization had to adopt more robust digital security practices, including limiting the methods by which staff share sensitive information, using more secure email, engaging in external security audits, and upgrading equipment; however, such measures are bound by resource constraints.[197] He stated that "there is an impact of fear" and a "transfer of energy. … We had to devote time, energy, resources" to the organization's surveillance response. He further reflected, "I think there is also a jolt, a wake-up call. We all make mistakes. We may have areas that are not so bright that we don't want to be public."[198]

115. Another journalist commented similarly, "Now journalists have to spend energy, time and money to protect themselves, instead of investigating, which is their job."[199]

116. Another journalist explained:

> After learning about Pegasus, we started having meetings. Our meetings were exclusively about this topic. There was also a call for us to change our relationship with technology. We could have the newest gadgets, but if we didn't change our relationship with technology, it wasn't going to be fully effective. And that we all had the awareness of how serious that was. That was the most relevant thing for me. I no longer have an electronic agenda, I am more cautious with the messages I leave in a chat room. This was one of the reasons why some journalists left the media outlet.[200]

117. In a clear manifestation of the potential of surveillance to undermine journalism and rights defense, the Special Rapporteurship has spoken with a number of individuals whose experience of surveillance resulted in their exile from their home state. Indeed, El Faro as an organization relocated to Costa Rica in 2023 in order to maintain its ability to engage in independent journalism.[201] Such exile is a form of censorship linked to surveillance, and creates numerous administrative, financial, mental, and physical hardships for those who are forced to leave.[202]

3. Surveillance results in significant intersectional and gender-based harms

118. The Special Rapporteur observes that the harms associated with surveillance technologies are frequently amplified when the surveilled individual is a member of a vulnerable group, including black, female, and LGBTQI+ persons. It is essential to recognize the unique manifestations of these individuals' surveillance experience, and the intersectional nature of the human rights impacts of surveillance. Indeed, as discussed in section II.A.3, the racial bias of facial recognition technologies is well documented. Additionally, the use of surveillance technologies against women, girls, and LGBTQI+ persons to gather information related to their sexuality or gender identity may expose them to risk of physical violence as well as legal or social repercussions.

119. Amnesty International has described the phenomenon of technology-facilitated gender-based violence as:

---

[197] Testimony No. 26, obtained on October 9, 2024.
[198] Testimony No. 26, obtained on October 9, 2024.
[199] Testimony No. 01 and 02, obtained on October 29, 2024.
[200] Testimony No. 04, obtained on October 9, 2024.
[201] El Faro, El Faro Moves to Costa Rica, April 13, 2023.
[202] See IACHR, Office of the Special Rapporteur for Freedom of Expression, Exile of journalists and freedom of expression, OEA/Ser.L/V /II CIDH/RELE/INF.30/25, April 15, 2025.

> any act of violence, or threats thereof, perpetrated by one or more individuals that is committed, assisted, aggravated and amplified in part or fully by the use of information and communication technologies or digital media, that disproportionately impacts women, girls and other people based on their real and/or perceived sexual orientation, gender identity and/or expression, causing physical, psychological, economic and sexual harm. Gender-based violence exists in a continuum between physical and digital spaces.[203]

120. Digital surveillance, including the use of spyware, can constitute a form of technology-facilitated gender-based violence when it instills fear or causes its targets to stay silent or withdraw from public discourse, thus chilling the freedom of expression and activism of women and LGBTQI+ human rights defenders.

121. Two interviews undertaken by the Special Rapporteurship with individuals who were targeted with Pegasus spyware reflected the particular harms associated with the use of surveillance technologies against LGBTQI+ persons. An opposition politician who was surveilled with Pegasus spyware described how, while attacks on the opposition were not new, the person felt that the strategy had shifted to discrediting the adversary not with debates, but with insults and dirty games. The person believed that methods to do harm have amplified in the country, and the Pegasus infection was just one example. The use of surveillance was particularly intrusive because the person had kept their sexual orientation private; after details about their relationship started to appear in the media, they felt compelled to make a public statement about both the surveillance and their sexual preferences. The person reflected that, while highlighting the importance of these issues was a positive outcome, the use of spyware itself was a violation of privacy and contributed to the fact that opposition voices were being silenced. The person felt they had engaged in self-censorship, and is in a situation of "permanent paranoia." The person has adopted enhanced digital security measures, and ultimately decided to leave the country and pursue a new career. The surveillance affected personal relationships as well. [204]

122. A journalist who identifies as bisexual felt similar pressure to go public about their sexual preference after their device was infected with Pegasus. When the infection happened, fewer than 10 people knew of the person's sexual orientation, and they were concerned that their private life would be revealed on the Internet. Faced with this situation, the person decided to make a public column and expose the issue, to avoid potential blackmail about their private life. The person felt the experience had a negative impact on mental health and created a "digital paranoia."[205]

123. The Special Rapporteurship also received extensive input during preparation of this report regarding the doubly hostile environment experienced by women, which reflects the use of surveillance technologies against them in combination with overarching campaigns of gender-based online (and in some cases offline) harassment and disinformation. According to a study by the Association for Progressive Communications (APC) of the experiences of women human rights defenders in Global South countries, women human rights defenders have been systematically targeted with digital surveillance.[206] For example, in Brazil:

---

[203] Amnesty International, Thailand: "Being ourselves is too dangerous": Digital violence and the silencing of women and LGBTI activists in Thailand, May 16, 2024, p. 10.

[204] Testimony No. 06, obtained on November 6, 2024.

[205] Testimony No. 15, obtained on October 24, 2024.

[206] Information submitted by Association for Progressive Communications (APC) in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, pp. 15-16, 18-19, 37-38.

> these intrusions often resulted in the unauthorized access and manipulation of private communications, leading to the spread of defamatory content aimed at discrediting their activism. For instance, one activist reported that her phone was hacked, and her social media accounts were used to post messages falsely portraying her as a "gold digger" and a "prostitute." This not only undermined her reputation but also caused significant psychological distress. Moreover, the ongoing nature of these threats suggests that the surveillance is not an isolated occurrence but part of a broader pattern of intimidation aimed at silencing dissent.[207]

124. APC also reported that women human rights defenders in Ecuador have similarly "been targets of digital violence, facing online harassment, surveillance, and defamation, often linked to their activism."[208] APC's study of women human rights defenders provided broad insight into the impacts of digital aggression that the women experienced, such as stress and fear in the face of threats and impunity; economic challenges; exhaustion and hopelessness; public discrediting; and family conflict.[209]

125. Such gender-based harms are also evident in the phenomenon of digital transnational repression, which utilizes surveillance and other digital threats to undermine the freedom of expression and activism of exiled and diaspora communities. A 2024 Citizen Lab study found:

> that exiled and diaspora women human rights defenders targeted through digital transnational repression face not only the same digital threats as men human rights defenders, but also gender-specific forms of online harassment, abuse, and intimidation. These threats lead to disproportionate harms that range from professional setbacks, stigmatization, and social isolation to the erosion of intimate relationships, profound emotional distress, and psychological trauma. Gender-based digital transnational repression also frequently involves the amplification and exploitation of entrenched patriarchal norms around women's bodies, sexuality, behavior, and notions of family honor, potentially leading to further forms of violence and discrimination.[210]

126. The interviews undertaken by the Special Rapporteurship reflected that the impacts of surveillance on female journalists and rights defenders frequently differ from, and are in some cases more severe than, those on their male colleagues. For example, one newspaper had worked to increase representation of female journalists in its ranks, but the spate of Pegasus infections within the organization undermined those efforts for gender parity: many of the staff who left the newspaper

---

[207] Information submitted by Association for Progressive Communications (APC) in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 16.

[208] Information submitted by Association for Progressive Communications (APC) in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 17.

[209] Information submitted by Association for Progressive Communications (APC) in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 38 ("Additionally, according to APC's ongoing study, WHRDs pointed out various types of impacts stemming from the digital aggressions they have experienced. On a personal level, they demonstrated prolonged stress due to the sense of impunity surrounding the violence. Fear arose in response to threats and the anonymity of the aggressors. Additionally, they experienced other emotional effects, such as feelings of hopelessness, persecution, collective exhaustion, and a pervasive fear of inadvertently causing harm to others. Significant economic challenges were perceived as well. These adversities not only hindered the WHRDs' ability to continue their work but also exacerbated their sense of vulnerability in the face of digital threats. "Impacts at the interpersonal and familial levels were detected, highlighting that digital attacks of a sexual nature, such as sexual defamation against one of the defenders in the area, had caused family conflicts with her partner. Likewise, defenders noted that some of the impacts of digital aggressions against individuals and their organizations had resulted in organizational economic setbacks, suspension of activities, discrediting in the public sphere, or exhaustion among all members").

[210] Citizen Lab, The Weaponization of Gender for the Purposes of Digital Transnational Repression, December 2, 2024.

were women, who felt different repercussions of surveillance than their male colleagues.[211] One journalist who left the country explained:

> I got information that the government was negotiating with the gangs. That's when I started to notice that my camera was turning on. At that moment I signed a note about the government's negotiations with the gangs. And that is why the threats were unleashed in networks.
>
> My boss told me not to leave my house so much. I was very "panicky." I was the only woman who signed that note.
>
> I had to go on a trip. The software was going in and out of my phone just as I was talking to my source.
>
> Then the microphone turned on. Then I panicked.
>
> The onslaught I was receiving on social media was overwhelming. So at the time I thought it might be my paranoia because of all the things they were saying to me on twitter.
>
> At the end of November I received an email from Apple that my phone was probably bugged with Pegasus. Later when I made my calendar of dates, I realized that they coincided with these key moments.
>
> I left the country in 2022…
>
> My family was very affected by the harassment, Pegasus, etc., it did affect a lot. Since November I stopped speaking out on social networks. My participation in twitter has decreased more and more, and I have restricted who can comment on my publications. I made my family download Signal to have communication.[212]

127. Another female journalist described having experienced misogynistic attacks online since 2019, in the context of the president's stigmatization of critical journalists. Such attacks included posts of pictures of herself and her daughters, as well as rape threats. "I thought about leaving the country because of the caliber of the threats." Many of her sources no longer wanted to speak with her, her career opportunities diminished, and her oldest daughter went to school abroad. Yet "Pegasus was the straw that broke the camel's back." After learning her device was infected with Pegasus spyware, she left the country.

> Before I found out about Pegasus, I had a lot of sources on the record. But after that I had a hard time… I had to rely on documentary sources, off the record. . . .
>
> The attack has been followed by anonymous accounts, troll farms, people who are very fanatic about following the government. These are the accounts that are now attacking me. The attacks they make are not about the quality of my work, but are misogynistic, sexualized, focusing on my body.

[211] Testimony No. 01 and 02, obtained on October 29, 2024.
[212] Testimony No. 05, obtained on October 9, 2024.

> I think there is a very big, very strong impact on a government's scope of work when there is a regime of fear and we know that we are being watched. Yes, it is very complicated. I admire very much those colleagues who have stayed in the country.

128. While she feels her situation has improved since leaving the country, she notes the need for constant vigilance: "Minimize risks and take nothing for granted."[213]

129. Another female journalist learned from a contact in the prosecutor's office that her photographs, chats, and information on her bank accounts had been displayed on a giant screen in the office, which shocked and horrified her. She reported feeling naked, unprotected, and violated.[214]

130. Another female journalist also emphasized that the risks faced by male and female journalists are distinct. On social media, many comments she received about her reporting were misogynistic; in this context, spyware that is capable of activating the camera of a device at will puts female journalists' privacy at serious risk. After experiencing a Pegasus infection, her physical and mental health as well as her personal relationships suffered severely. She felt a constant state of anxiety regarding the safety of her newspaper, and experienced sleep loss and other debilitating physical effects. She ultimately left the country, feeling that the country no longer had anything to offer her; being out of the country has proven "a great respite," allowing her to feel safer and healthier.[215]

131. A very similar experience was reported by an additional female journalist whose device was likewise infected with Pegasus within the context of ongoing, misogynistic online harassment campaigns against her. She felt that the online aggression amplified after the Pegasus infection: "I noticed a pattern of violence that increased, it was something staggered, the people [related to the government] sent hordes of trolls to attack." She self-censored in response. She no longer trusts digital devices. She also reported that she is much more aware of the safety of her family and loved ones, because if something happens to her, it affects the lives of others. She notes that this is an emotional burden that did not exist before the infection, but does now. She ultimately migrated, motivated by fears for her safety for her safety and her desire for a different model of life where she could live more peacefully, without government interference. In doing so she had to start over in her career, building new networks of contacts and finding any available work in her new country, with significant loss of income. While she has returned to the country to visit family, doing so causes her great fear: she feels she is permanently under surveillance, and "anything can happen."[216]

132. Notably, one female journalist pointed out that, among the group of people whose phones were infected with Pegasus, several of the women were asked by their families to resign. She herself felt the surveillance changed her relationship with her mother, who was very nervous for her safety and asked her not to work at the newspaper anymore; her grandmother likewise worried about her and asked her to look for another job. Her relationships with her friends were affected, as they could not communicate freely. The surveillance impacted her mental health, causing her anxiety, sadness, and a sense of paralysis, and she isolated herself. She stated that the surveillance

> was not something light, because I knew what it implied, and this happened because I was doing my job, because I was part of a team of journalists. It was hard

[213] Testimony No. 10A, obtained on October 8, 2024.
[214] Testimony No. 27, obtained on October 23, 2024.
[215] Testimony No. 09, obtained on October 9, 2024.
[216] Testimony No. 18, obtained on November 30, 2024.

> to process… I felt very angry, very upset, I thought it was unfair to be going through this infection. All for the simple fact of doing my job… Little by little I was shrinking.

133. She ultimately decided to leave the newspaper.[217]

134. Finally, in this context of pervasive gender-based surveillance harms and tactics of digital repression, the Special Rapporteur notes with particular concern the use of data brokers and location tracking tools to monitor women seeking healthcare services, recognizing the potential of these tools to significantly impact privacy, health and personal autonomy[218].

4. Surveillance impunity creates a state of continuous violation of the rights of targeted individuals

135. Specifically with respect to commercial spyware, accountability and remedy for the documented misuse of this category of invasive surveillance technologies have proven remarkably elusive. A key contributing factor to this impunity is the overarching lack of transparency surrounding state reliance on commercial spyware. States have asserted that such surveillance operations fall within national security or state secrecy exceptions to public reporting, and that revealing details of the use or procurement of commercial spyware would compromise law enforcement and intelligence.

136. Moreover, the technologies themselves are self-concealing, in two respects. First, they are technically designed to prevent detection or attribution, and to remove traces of use on a device. Second, when offered by private companies, the technical development and support of these technologies, as well as internal deliberations of the company with significant human rights implications, fall within the framework of commercial secrecy and outside the scope of public oversight.

137. Some individuals who have obtained evidence of spyware infection of their devices have pursued legal action.[219] Such efforts to obtain remedy through the courts have encountered numerous hurdles, including: jurisdictional challenges; limited access to or challenges against evidence or technical expertise; retaliation against the claimant or supporting experts in the form of legal or security threats or reputational attacks; and the significant financial costs associated with litigation.[220] While certain litigation is ongoing, individuals surveilled with commercial spyware have thus far been unable to obtain remedy through the courts.

138. For example, in Mexico, individuals monitored with Pegasus spyware filed criminal complaints with the Special Prosecutor's Office for Crimes Committed Against Freedom of Expression (FEADLE) in 2017, 2022, and 2023. These cases encountered numerous obstacles, including obstruction of the investigations, authorities' refusal to provide relevant records, and demands on the victims to relinquish their devices to authorities for the purported purpose of validating Pegasus

[217] Testimony No. 14, obtained on October 30, 2024.

[218] Privacy International, All Eyes on my Period? Period tracking apps and the future of privacy in a post-Roe world, May 28, 2025, How digital health apps can exploit users' data, March 4, 2022; The Conversation, Reproductive health care faces legal and surveillance challenges post-Roe – new research offers guidance, January 24, 2025; International Association of Privacy Professionals (IAPP), The state of US reproductive privacy in 2025: Trends and operational considerations, January 30, 2025; King's College London, Female health apps misuse highly sensitive data, study finds, May 13, 2024; Jo-Anne Patricia Hughson, J. Oliver Daly, Robyn Woodward-Kron, John Hajek, David Story, The Rise of Pregnancy Apps and the Implications for Culturally and Linguistically Diverse Women: Narrative Review, JMIR Mhealth Uhealth, November 16, 2018.

[219] See The Citizen Lab, Litigation and other formal complaints related to mercenary spyware, December 12, 2018.

[220] Interview with Access Now, October 2, 2024.

infections.[221] According to R3D, "What has happened is that investigations on surveillance abuses have become investigations of the victims, rather than the perpetrators."[222]

139. Moreover, the National Institute for Access to Information and Protection of Personal Data (INAI)–the autonomous national body charged with ensuring transparency of public information and data protection–made its own determinations that the Attorney General's Office improperly concealed contracts with NSO Group; and that the Secretariat of National Defense (SEDENA) must release its Pegasus-related contracts (a ruling also made by a federal judge in response to legal action by R3D).[223] Yet the Attorney General's Office made no serious effort to investigate the obstruction of justice, and SEDENA has refused to release its records.[224]

140. In November 2024, the Mexican legislature passed a measure eliminating INAI and several other autonomous watchdog agencies, thus reinforcing this climate of impunity.[225]

141. The only case in Mexico to progress to a stage in which judicial authorities ruled on illegal interception of communications was that related to the surveillance of journalist Carmen Aristegui. The case was brought against an individual operator within an intermediary company that facilitated the sale of NSO Group's Pegasus to the Attorney General's Office. While the judge validated the evidence of Pegasus infection that was presented, the case did not establish responsibility or advance accountability of the authorities, as the defendant was a private individual.[226]

142. Based on the monitoring carried out by this Office and reports received, surveillance abuses in El Salvador remain without adequate accountability. Certain members of *El Faro* whose devices were infected with Pegasus spyware were already the subject of precautionary measures granted by the IACHR in February 2021.[227] It is noteworthy that numerous Pegasus surveillance infections took place in months subsequent to the issuance of these precautionary measures, in clear contravention of the IACHR's resolution.[228]

143. In January 2022, the Association of Journalists of El Salvador (Asociación de Periodistas de El Salvador, or APES) filed notices with the Prosecutor's Office on behalf of a number of journalists whose devices were infected with Pegasus spyware.[229] At a March 2022 hearing of the IACHR regarding Pegasus spyware abuses in El Salvador, the Attorney General's office claimed it was

[221] Information submitted by R3D in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p.14-15; Interview with R3D, August 23, 2024.
[222] Interview with R3D, August 23, 2024.
[223] Information submitted by R3D in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p.14.
[224] Information submitted by R3D in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p.14; see also R3D, Ejército Espía.
[225] Reuters, Mexican senate passes proposal to abolish autonomous bodies, January 12, 2023; Mexico News Daily, Mexican Congress takes first step toward eliminating watchdog agencies, November 21, 2024.
[226] Information submitted by R3D in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 14, 31.
[227] IACHR, Resolution 12/2021, Precautionary Measure No. 1051-20, 34 identified members of the digital newspaper "El Faro" regarding El Salvador, February 4, 2021.
[228] The Citizen Lab, Project Torogoz: Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware - The Citizen Lab, January 12, 2022.
[229] Gato Encerrado, Apes presenta dos avisos a la Fiscalía para que investigue espionaje a periodistas, January 15, 2022.

investigating the situation.[230] Since then, individuals impacted have received no further information or contact from authorities about their cases.[231]

144. The NGO Cristosal also pursued legal action regarding the use of state funds for purchase of Pegasus spyware, which was used against its staff.[232] Their case, like the others, has not advanced and the institutions involved have refused to act.[233]

145. Given the lack of remedy for spyware abuses available in El Salvador, some members of El Faro brought legal claims against NSO Group in U.S. courts.[234] At the district level, the case was dismissed on grounds of *forum non conveniens*,[235] and the plaintiffs have appealed this ruling to the Ninth Circuit.[236] The outcome of spyware-related litigation in the US is significant; as EFF has noted: "All of the voluntary mechanisms established to hold spyware companies accountable have failed. US courts are the last viable venue for victims of surveillance and human rights abuses to vindicate their rights."[237] The Knight First Amendment Institute, which supported the El Faro plaintiffs in their action, affirmed that "U.S. courts have an important role to play here in safeguarding human rights, and holding spyware abusers accountable when spyware touches and concerns the U.S."[238]

146. Separately, technology providers whose platforms were exploited by spyware companies have brought suit.[239] In the United States, both WhatsApp Inc. and Apple Inc. sued NSO Group, the developer of Pegasus spyware, in relation to its unauthorized access to these companies' servers and exploitation of their respective products. The WhatsApp suit, filed in October 2019, survived a gauntlet of motion practice, and plaintiffs ultimately prevailed on their Computer Fraud and Abuse Act, California Comprehensive Computer Data Access and Fraud Act, and breach of contract claims in a ruling on summary judgment in December 2024.[240] The win was hailed by civil society as "the first major court victory against NSO Group in the world."[241] In May 2025, a jury awarded damages to WhatsApp in the amount of $167 million, and NSO Group moved for a new trial.[242] The Apple suit, filed in November 2021, was voluntarily dismissed on motion from Apple in November 2024, based on its concerns over the risk the discovery process could present to Apple's threat intelligence program.[243] As illustrated by the diverging approaches to litigation of these companies, however, suits brought by technology providers are at best a proxy for remedy to the individuals who are directly impacted by intrusive surveillance: the course of costly legal action will depend on the interests of the company, which may not be in perfect alignment with the interests of individuals who have experienced human rights impacts.

---

[230] IACHR, Hearing, La situación de los derechos humanos en el contexto de la vigilancia cibernética en El Salvador, 183rd Period of Sessions, March 16, 2022; Information submitted by Access Now in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 2-3.

[231] Information submitted by Access Now in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 2-3.

[232] Infobae, Demandan a ente salvadoreño que se negó a investigar compra de Pegasus, July 19, 2022; LatAm Journalism Review by the Knight Center, NGO to file injunction in El Salvador's Supreme Court over spying on journalists via Pegasus spyware, May 1, 2023.

[233] El Salvador, Cristosal: Gobierno ignora indagar espionaje con Pegasus, April 28, 2023.

[234] Knight First Amendment Institute at Columbia University, Dada v. NSO Group: a case challenging the use of spyware against journalists.

[235] Knight First Amendment Institute at Columbia University, Dada v. NSO Group, March 8, 2024.

[236] Knight First Amendment Institute at Columbia University, Dada v. NSO Group: a case challenging the use of spyware against journalists.

[237] Interview with EFF, July 31, 2024.

[238] Interview with Knight First Amendment Institute, August 12, 2024.

[239] The Citizen Lab, Litigation and other formal complaints related to mercenary spyware, December 12, 2018.

[240] Casetext, WhatsApp Inc. v. NSO Grp. Techs.

[241] Access Now, Statement on the historic decision in the WhatsApp v NSO case, January 13, 2025.

[242] Tech Crunch, NSO Group asks judge for new trial, calling $167 million in damages 'outrageous', June 2, 2025.

[243] Court Listener, Apple Inc. v. NSO Group Technologies Limited, March 29, 2025.

147. Pursuit of remedy in cases of spyware abuse raises complex considerations. As Access Now has noted, "What is an adequate remedy in itself? You can't really make a victim whole in this case when their privacy is taken from them, violated in such a way. Remedy hasn't been obtained in the legal cases thus far."[244]

148. At the same time, the benefits of legal action are not limited to obtaining a favorable judgment or award of damages. According to Access Now, "Victims want to be heard about the harms that were inflicted on them, and feel as active participants in these cases; they often feel like things are just happening to them and they have no power, no say, no control. It is very disempowering. At least having their voices heard in these processes to make clear that they were impacted, is another objective that victims have."[245] EFF similarly stated, "Plaintiffs don't necessarily want money, they want *some* legitimate forum, *some* adjudicator to say yes this is wrong, this is a violation of rights. The ultimate goal is for these abuses to stop."[246] "Even if there was no actionable remedy available, just a *finding* alone is still better than nothing, even if that is an incomplete remedy."[247]

149. Legal action is also one of the few avenues available to obtain greater transparency about state use of commercial spyware. Access Now points out: "The hope is that through legal cases there will be an opportunity to uncover some of that information, such as procurement and use of that technology by particular agencies, what agencies are using spyware, how the use was approved, whether there was a legal basis, whether the law was followed. This is important for victims themselves as well as others not participating in the case."[248]

150. Given the risks and hurdles associated with seeking remedy through the courts, however, some individuals who have experienced spyware infections have noted that they do not feel pursuing remedy is worthwhile and could in fact subject them to further harm. Access Now made the following assessment:

> "Working with spyware victims is very similar to working with victims of physical violence: the psychological impact is similar, but in a way it is worse. In cases of spyware the assailant is a powerful state with so much resource and power, it is challenging to resist it. This makes some victims reluctant to come forward, reveal names, participate in legal accountability measures, because of the risk of retaliation. In criminal cases we were able to issue restraining orders, ensure victims' protection, but in cases of states [surveilling individuals] that is not possible. These are very challenging cases from that perspective."[249]

151. Indeed, a number of individuals with whom the Special Rapporteurship spoke confirmed this sense of futility and risk. A human rights defender pointed out that, regarding the use of Pegasus spyware against himself and others, "impunity is so palpable.. There are no consequences, the State does not investigate, does not guarantee rights, and commits actions against its population–and with all this there are no consequences."[250]

[244] Interview with Access Now, October 2, 2024.
[245] Interview with Access Now, October 2, 2024.
[246] Interview with EFF, July 31, 2024.
[247] Interview with EFF, July 31, 2024.
[248] Interview with Access Now, October 2, 2024.
[249] Interview with Access Now, October 2, 2024.
[250] Testimony No. 13, obtained on October 28, 2024.

152. Another journalist stated, "We do not feel safe to ask for protection from the government we suspect is the main executor of this espionage." Even so, he and other journalists attempted to work with the prosecutor's office to pursue accountability for the surveillance, but the investigation failed to progress. "There was ignorance and lack of interest in the subject. They only wanted to say 'Yes, we listen to the victims.' They had not even read the complaint properly. It was an evident disinterest, even wanting us to notice it."[251]

153. One journalist explained that she chose not to report her Pegasus infection to the relevant prosecutor: after consulting with her family, she decided that she "was the one who would lose out" and felt it would amount only to an additional emotional burden.[252]

154. A human rights defender described a situation of having been infected with spyware in two separate attacks, "in two different moments, by two different governments, both denounced without any progress in terms of justice. We think that the recidivism in our case is very illustrative of the fact that when there is no justice, when there is no investigation, it happens again."[253] Another member from the same human rights organization added that reporting both attacks and pursuing accountability felt like "the right thing to do. But what the first complaint had proven to us was that it was not going to move forward."[254] These human rights defenders identified that obstacles to accountability included a lack of independence of the investigators; lack of coordination between institutions; poor inter-institutional coordination; limited international cooperation and resistance to external technical assistance; as well as insufficient technical capacity within the relevant institutions, rejection of independent expertise, failure to consider contextual factors, non-cooperation by state entities, and the misuse of national security arguments to block transparency.[255]

155. The lack of investigation, absence of effective remedies, and overarching impunity serve as further catalysts to the normalization of surveillance practices, creating a permissive environment for continuous human rights violations. Failures to investigate and provide reparations perpetuate systematic human rights abuses.

156. Ultimately, the impunity demonstrated with respect to spyware abuses runs counter to the state obligation to guarantee the right to effective remedy for human rights violations.[256] As elaborated by the Inter-American Court of Human Rights, "the State has a legal duty to take reasonable steps to prevent human rights violations and to use the means at its disposal to carry out a serious investigation of violations committed within its jurisdiction, to identify those responsible, to impose the appropriate punishment and to ensure the victim adequate compensation."[257] These duties remain unfulfilled in existing cases of spyware abuse.

157. Moreover, the NGO R3D highlights the similarities between harms felt within the context of impunity for spyware abuses, and the harms associated with enforced disappearances, in that both result in continuous, ongoing harm.

---

[251] Testimony No. 03, obtained on September 30, 2024.
[252] Testimony No. 27, obtained on October 23, 2024.
[253] Testimony No. 26, obtained on October 9, 2024.
[254] Testimony No. 26, obtained on October 9, 2024.
[255] Testimony No. 26, obtained on October 9, 2024.
[256] International Covenant on Civil and Political Rights, New York, United States of America, 1966, art. 2(3); American Convention on Human Rights, San José, Costa Rica, 1969, art. 1(1).
[257] Inter-American Court of Human Rights (IACtHR). Case of Velásquez-Rodríguez v. Honduras. Merits. July 29, 1988, para. 174.

> "As long as surveillance is not remedied by providing the victims with truthful information about who spied on them, why, and what information was obtained, how it was used — the pain of the victims doesn't stop. Even when surveillance ceases they continue to feel the effects of this surveillance, wondering if intelligence will be used to embarrass them, engage in influence operations, make attempts on their lives, or create other adverse consequences for them. This is a continued violation… After years of being with people who are surveilled, they continue to suffer. It is similar to [cases of] disappearances: as long as you don't know where your loved one ended up, you don't have any peace."[258]

158. The lack of clarity or recourse surrounding the misuse compounds the harm experienced by those surveilled. Access Now has described the impact as follows: "Now you have to wonder what information do they have? [Victims] operate under the presumption that all information in their phone was accessible to the government. At any point that information could be used against you, your associates, your sources. This is something individuals who have been targeted have to constantly worry about, and think about what they say, what they do."[259]

159. A journalist who spoke with the Special Rapporteurship recounted feeling she was in a state of defenselessness: "Who can stop this from happening? That is something difficult to answer, because it is not like turning off a switch, it is such a serious and intangible fact, it is a feeling of being unprotected. I always think that there could be another infection, even though I no longer work at the newspaper." She felt the infection made clear that nothing was guaranteed, particularly given that this type of spyware is constantly evolving.[260]

160. A journalist infected with Pegasus remarked,

> I may be handling myself with certain precautions. But I assume that there is a follow-up… we know that they are trying to find our "Achilles heel." All this has led me to continue taking precautionary measures that allow me to enter territories, to contact my sources, leaders who handle first-hand information, but in a safe way. So that I do not have to expose the person and not expose myself. If they connect with media and journalists, they may run the risk of being detained under the emergency regime. The regime aggravates the situation. We have to be more careful how we handle communication. It is more and more necessary to think about being a little more radical in some of the measures we were already taking, but thinking about the direction our country is going … We have to keep thinking about how to protect ourselves.[261]

161. As another journalist emphasized, it is important to her to know who was behind the infection, what information they collected, and what they did with the information. She would like to see guarantees of non-repetition for such surveillance, pointing out that she and her colleagues should be certain that their private life is private, as are their sources.[262]

[258] Interview with R3D, August 23, 2024.
[259] Interview with Access Now, October 2, 2024.
[260] Testimony No. 14, obtained on October 30, 2024.
[261] Testimony No. 08, obtained on October 1, 2024.
[262] Testimony No. 09, obtained on October 9, 2024.

162. Another journalist similarly stated that one of his main fears is not knowing what was taken from his phone or who has it. He is particularly concerned that someone must have photos of his family, as they have had access to his private life, and about how information taken from him could harm his family. "Beyond the theoretical, that is, realizing that you've been exposed, naked for a long time, you do feel naked because you've been stripped, because privacy is a right... At first you don't dimension, but tell us, and give us back what they took, because it's mine."[263]

163. The Special Rapporteur agrees that, a state's refusal to disclose facts or acknowledge the commission of misuse of intrusive spyware effectively places the victim outside of the protection of the law, preventing as it does genuine accountability or access to remedy. Moreover, a state's act of intrusive surveillance should be considered a continued human rights violation as long as the perpetrators continue to conceal the facts regarding the information extracted (e.g., type of data [work, personal, intimate, financial], scope of use, retention and destruction) and "these facts remain unclarified."[264] As the Inter-American Court observed in *CAJAR*, "the existence and retention of intelligence files containing personal data" constitutes a "permanent interference with the right to privacy."[265] The harm of intrusive surveillance is not mitigated without the transparent expungement of exfiltrated data and enforceable guarantees of non-repetition.

[263] Testimony No. 16, obtained on October 31, 2024.

[264] United Nations (UN), General Assembly, Declaration on the Protection of all Persons from Enforced Disappearance, resolution 47/133, December 18, 1992, art. 17.

[265] IACtHR. Case of Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" v. Colombia. Preliminary Objections Merits, Reparations and Costs. October 18, 2023, para. 580.

II. REGIONAL AND INTERNATIONAL LEGAL FRAMEWORK

164. At this stage of the international effort to curb surveillance abuses, informed by years of research, reporting, and advocacy regarding human rights, the legal and normative standards applicable to the use of digital surveillance and the operation of the surveillance market are well explored.[266] The Special Rapporteurship notes that digital surveillance implicates a host of rights,[267] and has fundamentally threatened the rights to freedom of opinion and expression and to privacy, which itself underpins freedom of expression.[268] The International Covenant on Civil and Political Rights (ICCPR) protects the rights to freedom of opinion and expression and to privacy,[269] as does the American Convention on Human Rights (American Convention).[270] As is well established, states may only restrict the rights to freedom of expression and privacy in compliance with the principles of legality, necessity and proportionality, and legitimate aim,[271] while the right to hold an opinion without interference is absolute and not subject to restriction.[272]

165. Additionally, the Special Rapporteurship emphasizes that state use of mass surveillance is presumptively incompatible with human rights norms. As UN bodies and experts[273] as well as this Rapporteurship[274] have emphasized, mass surveillance by States is inherently disproportionate and thus cannot meet the requirements of international human rights law.

166. The Inter-American system has further refined the legal framework applicable to state surveillance practices, and advanced understanding of the impact of such practices on human rights. Indeed,

---

[266] See, e.g., UN, General Assembly, Human Rights Council, Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/51/17, August 4, 2022; UN, General Assembly, Resolution 73/179: The right to privacy in the digital age, A/RES/73/179, adopted on 17 December 2018; UN, General Assembly, Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/41/35, May 28, 2019; UN, General Assembly, Human Rights Council, Report of the United Nations High Commissioner for Human Rights, A/HRC/39/29, August 3, 2018 ; UN, General Assembly, Human Rights Council, Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37, June 30, 2014; UN, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/23/40, April 17, 2013; Council of Europe, Venice Commission, Report on a rule of law and human rights compliant regulation of spyware, December 13, 2024, section III.

[267] See UN, General Assembly, Human Rights Council, Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37, June 30, 2014, para. 14; European Parliament, Surveillance and censorship: The impact of technologies on human rights. April 2015, section 2.3.

[268] "[T]he exercise of the right to privacy is important for the realization of the right to freedom of expression and to hold opinions without interference, and is one of the foundations of a democratic society" (UN, General Assembly, Resolution 68/167: The right to privacy in the digital age, A/RES/68/167, adopted on December 18, 2013); "Privacy and expression are intertwined in the digital age, with online privacy serving as a gateway to secure exercise of the freedom of opinion and expression." (UN, General Assembly, Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/41/35, May 28, 2019, para. 24).

[269] International Covenant on Civil and Political Rights, New York, United States of America, 1966, articles 19 and 17, respectively.

[270] American Convention on Human Rights, San José, Costa Rica, 1969, articles 13 and 11, respectively.

[271] UN, General Assembly, Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/41/35, May 28, 2019, para. 24; The Necessary and Proportionate Principles, developed by a coalition of civil society, privacy, and technology experts, aid in clarifying the application of international human rights law to communications surveillance, including within the Inter-American system. As laid out therein, elements of rights-compliant surveillance operations include independent judicial authorization, due process, user notification, public oversight, and transparency.

[272] UN, General Assembly, Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, A/HRC/29/32, May 22, 2015, paras. 19-21; IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections Merits, Reparations and Costs. October 18, 2023. Series C No. 506, para. 528 et seq.

[273] Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc A/69/397, September 23, 2014 – See also paragraphs 52, 59, and 63; Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29, August 3, 2018, paras. 17-18; Concluding Observations on the Third Periodic Report of Lebanon, Human Rights Committee, UN Doc CCPR/C/LBN/CO/3, May 9, 2018, paras. 33-34.

[274] UN, OSCE, OAS, ACHPR, Joint Declaration on Freedom of Expression and Responses to Conflict Situations, May 4, 2015, para. 8(a); IACHR, Office of the Special Rapporteur for Freedom of Expression, Standards for a Free, Open, and Inclusive Internet, OEA/Ser.L/V/II, CIDH/RELE/INF.17/17, March 15, 2017, para. 222.

the Inter-American system considers the right to freedom of expression of vital importance. The Inter-American Court of Human Rights (the "Court") has emphasized that the expansive language of Article 13 of the American Convention reflects the "extremely high value that the Convention places on freedom of expression. A comparison of Article 13 with the relevant provisions of the European Convention (Article 10) and the Covenant (Article 19) indicates clearly that the guarantees contained in the American Convention regarding freedom of expression were designed to be more generous and to reduce to a bare minimum restrictions impeding the free circulation of ideas."[275] The right to freedom of expression is further reinforced in the IACHR's Declaration of Principles on Freedom of Expression[276] and the Inter-American Democratic Charter.[277]

167. Article 13(3) of the American Convention is of unique relevance to state use of surveillance technologies. It includes parameters additional to those established by the ICCPR regarding restrictions on the right to freedom of expression, providing:

> The right of expression may not be restricted by *indirect methods or means*, such as the *abuse of government or private controls over* newsprint, radio broadcasting frequencies, or *equipment used in the dissemination of information, or by any other means tending to impede the communication and circulation of ideas and opinions* (emphasis added).[278]

168. At the outset, Art. 13(3) specifically identifies abuse of government or private controls over communications equipment as a prohibited restriction of the right to freedom of expression. Many advanced spyware technologies, such as NSO Group's Pegasus, provide the state with full access to and operational control over digital communications devices, which are regularly used to disseminate information. Abuse of such technology falls explicitly within the enumerated prohibition of Art. 13(3).

169. Moreover, it quite broadly prohibits any method or means used by the state to "effectively restrict, even if indirectly, the communication of ideas and opinions;"[279] the operative factor is the restrictive *effect* of the state activity. The Court interpreted the placement of this article as indicative of "a desire to ensure that the language … [regarding permissible restrictions] not be misinterpreted in a way that would limit, except to the extent strictly necessary, the full scope of the right to freedom of expression."[280] Moreover, this provision clarifies that states have an obligation to ensure that

[275] IACtHR. Compulsory Membership in an Association Prescribed by Law for the Practice of Journalism (Arts. 13 And 29 American Convention On Human Rights). Advisory Opinion Oc-5/85. November 13, 1985. Series A No. 5, para. 50.

[276] "Prior censorship, direct or indirect interference in or pressure exerted upon any expression, opinion or information transmitted through any means of oral, written, artistic, visual or electronic communication must be prohibited by law. Restrictions to the free circulation of ideas and opinions, as well as the arbitrary imposition of information and the imposition of obstacles to the free flow of information violate the right to freedom of expression." (IACHR, Declaration of Principles on Freedom of Expression, adopted by the IACHR at its 108th regular session held from October 2 to 20, 2000).

[277] "Transparency in government activities, probity, responsible public administration on the part of governments, respect for social rights, and freedom of expression and of the press are essential components of the exercise of democracy. The constitutional subordination of all state institutions to the legally constituted civilian authority and respect for the rule of law on the part of all institutions and sectors of society are equally essential to democracy." (Inter-American Democratic Charter, Lima, Perú, 2001, art. 4).

[278] American Convention on Human Rights, San José, Costa Rica, 1969, art. 13(3).

[279] IACtHR. Case of Ríos et al. v. Venezuela. Preliminary Objections, Merits, Reparations, and Costs. January 28, 2009. Serie C No. 194, para. 340.

[280] IACtHR. Compulsory Membership in an Association Prescribed by Law for the Practice of Journalism (Arts. 13 And 29 American Convention On Human Rights). Advisory Opinion Oc-5/85. November 13, 1985. Series A No. 5 para. 47.

violations of the right to freedom of expression do not result from private controls,[281] which obligation is also reflected in the UN Guiding Principles on Business and Human Rights.[282]

170. As the past years of research, reporting, and litigation regarding the use of surveillance technologies have shown, it is challenging and in many cases impossible for individuals to obtain direct evidence of a state's use of digital surveillance against them. Nevertheless, pursuant to Art. 13(3), the analysis extends beyond proving specific surveillance incidents. The key factor is not only the precise incident of surveillance but the overall restrictive effect of a pervasive climate of surveillance. A track record of surveillance abuse by a state, whether in the form of cyber-patrolling, misuse of facial recognition technologies, the use of commercial spyware against civil society, or other reported abuses, inevitably creates a public climate of digital distrust, which effectively restricts expression as individuals – particularly those within vulnerable populations – self-censor, or otherwise limit and modify their digital engagement. States with entrenched records of widespread surveillance abuse may thus presumptively run afoul of Art. 13(3).

171. This conclusion is further reinforced by the IACHR's Declaration of Principles on Freedom of Expression, which explicitly prohibits "direct or indirect interference in or pressure exerted upon any expression, opinion or information transmitted through any means of oral, written, artistic, visual or electronic communication." The Declaration's Principle 5 establishes that such indirect interference must be "prohibited by law" and that "restrictions to the free circulation of ideas and opinions, as well as the arbitrary imposition of information and the imposition of obstacles to the free flow of information violate the right to freedom of expression."[283]

172. Moreover, Principle 13 of the Declaration specifically addresses "indirect pressures exerted upon journalists," recognizing that such pressures constitute violations of freedom of expression even when they do not involve direct censorship. The pervasive climate of digital surveillance documented in this report operates precisely as such an "indirect pressure," creating conditions where journalists, human rights defenders, and civil society actors modify their behavior, sources, and communications to avoid potential surveillance targeting. This aligns with the Declaration's recognition that freedom of expression can be violated not only through direct restrictions but also through the creation of environments that inhibit the free circulation of ideas and information.

173. Adherence to this framework in the context of surveillance requires states in the Americas to develop strict norms and laws, policies and practices, that ensure *restraint* and *transparency* in state practice, to prevent surveillance mechanisms from directly or indirectly impinging on the right to freedom of expression. States must actively work to repair public trust in the digital environment, which has eroded as the result of state and private sector overreach. Approaches to that end could include, for example, strengthened data protection laws, establishment and support of independent surveillance authorization and oversight mechanisms, reliance on least intrusive means for data collection and surveillance, and robust disclosure regarding surveillance capabilities, surveillance deployment, and compliance with legal frameworks for surveillance.

---

[281] IACtHR. Compulsory Membership in an Association Prescribed by Law for the Practice of Journalism (Arts. 13 And 29 American Convention On Human Rights). Advisory Opinion Oc-5/85. November 13, 1985. Series A No. 5, para. 48; "Additionally, Article 13(3) of the Convention imposes of the State obligations to guarantee, even in the realm of the relationships between individuals, since it not only covers indirect governmental restrictions, but also 'individual...controls' that produce the same result." (IACtHR. Case of Ríos et al. v. Venezuela. Preliminary Objections, Merits, Reparations, and Costs. January 28, 2009. Serie C No. 194, para. 340).

[282] UN, General Assembly, Human Rights Council, Guiding Principles on Business and Human Rights, HR/PUB/11/04, 2011, Principle 1.

[283] IACHR, Office of the Special Rapporteur for Freedom of Expression, Background and Interpretation of the Declaration of Principles, 2000.

174. While States within the region have developed domestic legal frameworks[284] applicable to the use of surveillance and the collection of personal data, significant human rights challenges remain.[285] It is reported that in the Americas, even those States with legal frameworks providing some form of judicial review of surveillance measures suffer from loopholes and exceptions in the law; lower standards of protection for metadata; and an overarching lack of transparency, safeguards, accountability mechanisms, independence in oversight, and separation of powers.[286] Regional civil society organizations have documented how existing legal frameworks are frequently "outdated" and "insufficient" to address the human rights implications of modern surveillance technologies and provide guarantees to victims.[287] The rapid pace of technological change has enabled States to acquire and implement surveillance technologies that pose serious risks to human rights, while authorization and oversight mechanisms designed for traditional surveillance methods have proven inadequate for addressing the scope and intrusiveness of modern digital surveillance technologies.

175. It is in this context that the Inter-American Court's decision in *CAJAR* provides much-needed legal clarity. As discussed in Section V.A below, the decision enumerates the criteria by which States and the international community may assess the validity and legitimacy of State surveillance operations. Beyond that analysis, the Court developed the right to informational self-determination as grounded in the rights to protection of honor and access to information (Articles 11 and 13), and judicial protection (Article 25). The Special Rapporteur considers that this landmark judgment expands the Inter-American understanding of how surveillance impacts human rights beyond the traditional framework of privacy and freedom of expression.

176. The Court's recognition of the right to "informational self-determination" represents a crucial evolution in Inter-American human rights jurisprudence, drawing on decisions of national courts in the region and other precedent. This right, which the Court anchored in Articles 11 and 13 of the American Convention, encompasses not merely the protection of personal data but the broader capacity of individuals to control how their personal information is collected, processed, stored, and used by state authorities. The Court viewed the right as essential to "guarantee [individual] autonomy and freedom to self-determine."[288] As the Court explained, this right incorporates within its essential content, the right to access and control personal data in the possession of any public organ, and operates equally with respect to registries or databases in the hands of private parties.[289]

177. In the context of digital surveillance documented in this report, informational self-determination is crucial. The Court's analysis in *CAJAR* demonstrates that states cannot simply collect and retain

[284] Information submitted by the OAS Permanent Missions of Ecuador, Argentina and Mexico in response to the request for information by the IACHR Office Special Rapporteur for Freedom of Expression, 2024.

[285] Information submitted by Electronic Frontier Foundation (EFF) in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, September 2024, pp. 10-20; Information submitted by El Veinte in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, 2024; Information submitted by Fundación Karisma in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024.

[286] Information submitted by Electronic Frontier Foundation (EFF) in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, September 2024, pp. 18-21; Information submitted by Access Now in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, pp. 5-6; Information submitted by Association for Progressive Communications (APC) in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 42; Information submitted by R3D in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, pp. 26-29; Interview with SocialTIC, August 19, 2024.

[287] Information submitted by Fundación Karisma in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 23.

[288] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections, Merits, Reparations and Costs. October 18, 2023. Series C No. 506, para. 585.

[289] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia, Official Summary issued by the Inter-American Court, p. 7.

personal information indefinitely; individuals must have effective means of knowing what data is held and how it was obtained, as well as to request updating, rectification or modification of information or, if legally possible, its elimination.[290] The absence of such mechanisms in surveillance operations creates a permanent state of rights violation.[291] In essence, the right to informational self-determination counters both the lack of transparency and the inability to access remedy that facilitate and perpetuate surveillance abuses.

178. The Court also recognized "the right to defend human rights" as an autonomous right that can be violated independently of other rights violations. As the Court stated: "it is feasible, through an evolutionary interpretation of [the American Convention's] provisions, to derive recognition of a right, properly speaking, to defend human rights."[292] This right "incorporates the effective possibility of freely exercising, without limitations and without risks of any kind, different activities and work aimed at promoting, monitoring, promoting, disseminating, teaching, defending, claiming or protecting universally recognized human rights and fundamental freedoms."[293] The Court highlighted "the importance of the role played by human rights defenders in a democratic society… [A]ctivities carried out by human rights defenders contribute in an essential way to the observance of human rights, insofar as they act as guarantors against impunity and, in turn, complement the role of the States and of the Inter-American System as a whole."[294]

179. This autonomous character is crucial for understanding surveillance targeting of human rights defenders, journalists, and civil society actors. When states deploy surveillance technologies specifically because individuals engage in human rights work—as documented in this report—they violate not only privacy and freedom of expression, but the fundamental right to defend human rights itself. The Court emphasized that "the imposition of illegitimate limitations or obstacles to develop such activities in a free and safe manner by human rights defenders, precisely because of their condition as such and the work they carry out, may entail the violation of the right."[295] Moreover, the Court noted that the right to defend human rights imposes on states a special duty of protection of defenders, including ensuring a safe and enabling environment and investigating attacks, threats, or intimidation against defenders.[296]

180. The Special Rapporteurship also notes that the concurring opinion in *CAJAR* points toward recognition of what might be termed a "right to systems integrity"—the right of individuals to maintain the security and integrity of their digital devices and communications systems against unauthorized access—as a logical consequence of the right to informational self-determination. While not explicitly articulated as such, this right emerges from the Court's analysis of how

[290] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections, Merits, Reparations and Costs. October 18, 2023. Series C No. 506, para. 582.
[291] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections, Merits, Reparations and Costs. October 18, 2023. Series C No. 506, para. 580.
[292] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections, Merits, Reparations and Costs. October 18, 2023. Series C No. 506, para. 977.
[293] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections, Merits, Reparations and Costs. October 18, 2023. Series C No. 506, para. 978.
[294] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections, Merits, Reparations and Costs. October 18, 2023. Series C No. 506, para. 973.
[295] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections, Merits, Reparations and Costs. October 18, 2023. Series C No. 506, para. 978.
[296] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections, Merits, Reparations and Costs. October 18, 2023. Series C No. 506, para. 979.

intelligence activities violated multiple rights through unauthorized access to communications, infiltration of security schemes, and comprehensive monitoring of digital activities.[297]

181. In the digital context, the security of personal devices and communications systems is crucial to the exercise of numerous other human rights. When States deploy sophisticated spyware to gain full access to and operational control over a digital device, they compromise not only the specific communications accessed but the entire digital environment necessary for secure exercise of rights. This systemic compromise creates what could be characterized as a violation of systems integrity that enables ongoing violations of multiple other rights: "improper access to these systems as such (e.g. to a smartphone's hard drive or to someone's account on a cloud service) is particularly intrusive to individual autonomy, as it can cause significant risks and even harm to the fundamental rights and freedoms of the data subjects."[298] The emergence of a right to systems integrity calls for serious attention by states and the private sector to the human rights impacts of offensive stockpiling and use of vulnerabilities, and development of vulnerability equities processes that integrate human rights standards and perspectives.

182. The Court's holistic approach in *CAJAR* demonstrates that digital surveillance abuses cannot be understood in isolation. The judgment reveals how surveillance operates as a "continuing offense" that creates permanent conditions for rights violations. As the Court noted, intelligence activities created detailed profiles including "psychological profiles that described personality traits, behavior, interpersonal relationships and moods of those who were the object of intelligence activities."[299] This comprehensive profiling capability, enabled by modern digital surveillance technologies, violates what the Court characterized as the "full development of personality" protected by the American Convention.[300] When States can continuously monitor, profile, and predict individual behavior through digital surveillance, they alter the relationship between citizen and state, transforming surveillance from an exceptional measure into a tool of social control incompatible with democratic governance.

183. The Special Rapporteur emphasizes that these elements—informational self-determination, the right to defend human rights, and systems integrity—all flow from what the Inter-American Court recognizes as the foundational principle of personal autonomy. This Office observes that digital surveillance undermines what the Inter-American system recognizes as the cornerstone of human dignity: personal autonomy. As the Court emphasized, the American Convention "contains a universal clause for the protection of human dignity, which places the individual as both subject and end of the legal, political and social order, and provides content to both the notion of individual autonomy and the principle that guarantees that all persons must be treated as equals."[301]

184. According to Inter-American jurisprudence, personal autonomy encompasses "the possibility of every human being to self-determine and freely choose the options and circumstances that give

[297] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections, Merits, Reparations and Costs. October 18, 2023. Series C No. 506, Concurring Opinion of Judge Rodrigo Mudrovitsch, paras. 149-160.

[298] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections, Merits, Reparations and Costs. October 18, 2023. Series C No. 506, Concurring Opinion of Judge Rodrigo Mudrovitsch, para. 151.

[299] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections, Merits, Reparations and Costs. October 18, 2023. Series C No. 506, para. 343..

[300] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections, Merits, Reparations and Costs. October 18, 2023. Series C No. 506, para. 568.

[301] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections, Merits, Reparations and Costs. October 18, 2023. Series C No. 506, para. 567.

meaning to their existence, according to their own choices and convictions."[302] This principle "prohibits any state action that seeks the instrumentalization of the person, that is, that converts them into a means for purposes alien to choices about their own life and the full development of their personality."[303] As the Court explained in *CAJAR*, "in that context of autonomy and free development of personality, the person is also free to self-determine in order to decide when and to what extent they reveal aspects of their private life, which includes defining what type of information, including their personal data, can be known by others."[304]

185. Recognizing these substantive rights violations, the SRFOE underscores the importance of the right to an effective remedy, as enshrined in Article 25 of the American Convention. This right requires that individuals have access to simple, prompt, and effective recourse for protection of their fundamental rights.

186. The absence of notification mechanisms in surveillance operations, combined with the demonstrated lack of access to information regarding state surveillance, effectively renders the right to remedy illusory. Without knowledge of surveillance targeting, individuals cannot challenge the legality of state actions, seek accountability for abuses, or obtain information about the scope of data collected and its subsequent use. This creates a violation of Article 25 of the American Convention, runs counter to the aforementioned right to informational self-determination, and undermines the entire architecture of human rights protection in the digital ecosystem.

187. In the context of digital surveillance, the right to an effective remedy necessarily encompasses a derivative right to notification, as individuals cannot seek remedy for violations they do not know have occurred. States have a positive obligation to inform individuals subjected to surveillance—once it no longer jeopardizes the legitimate purpose—of the fact, legal basis, scope, and any available remedies.[305] This principle, established in European Court of Human Rights jurisprudence, recognizes post-facto notification as both a necessary safeguard against abuse of surveillance powers and a critical component of securing the right to an effective remedy.[306]

188. The Special Rapporteur concludes that the derivative right to notification must include not only notice of the fact of surveillance but also information about the legal basis for the surveillance, the scope of data collected, the duration of surveillance activities, and the measures taken to protect the collected data. Only through such comprehensive transparency mechanisms can individuals meaningfully exercise their right to seek remedy and ensure that surveillance activities comply with international human rights law.

189. Additionally, the Inter-American system's standards on access to information provide essential legal grounding for enhancing transparency to address surveillance abuses. Article 13 of the

[302] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections, Merits, Reparations and Costs. October 18, 2023. Series C No. 506, para. 569.
[303] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections, Merits, Reparations and Costs. October 18, 2023. Series C No. 506, para. 569.
[304] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections, Merits, Reparations and Costs. October 18, 2023. Series C No. 506, para. 570.
[305] Information submitted by Amnesty International's Security Lab in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, May 2025.
[306] European Court of Human Rights, Szabó and Vissy v. Hungary, Application No.37138/14, Judgment of 12 January 2016, para. 86; Weber and Saravia v. Germany, Application No. 54934/00, Decision of 29 June 2006, para. 135; Roman Zakharov v. Russia, Application No. 47143/06, Judgment of 4 December 2015, para. 287. See also European Parliament, Recommendation of 15 June 2023 to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (2023/2500(RSP)) (P9_TA(2023)0244), 15 June 2023, recommendations (h) and (i).

American Convention has been interpreted to include a right of access to information held by the state, which is essential for democratic accountability and oversight of surveillance practices[307]. The IACHR's Declaration of Principles on Freedom of Expression establishes that "access to information held by the state is a fundamental right of every individual" and that states have obligations "to guarantee the full exercise of this right."[308]

190. As documented throughout this report, the power imbalance created by states' refusal to disclose information about surveillance capabilities, deployment, and oversight prevents meaningful accountability and enables continued human rights abuses. In this regard, the Special Rapporteur observes that the OAS Model Inter-American Law on Access to Public Information,[309] as well as the Global Principles on National Security and the Right to Information (the Tshwane Principles),[310] could provide concrete guidance for Member States to fulfill their transparency obligations while protecting legitimate national security interests through narrow, time-limited exceptions subject to public interest balancing tests.

191. Building on the international human rights framework outlined above, the Special Rapporteur observes that states have consistently invoked national security and state secrecy doctrines to shield surveillance operations from scrutiny, effectively immunizing surveillance abuses from legal challenge. This approach contradicts the principle that there can be no areas of state activity entirely exempt from human rights oversight[311] As this Office documented in its 2020 thematic report on Access to Information and National Security, significant challenges persist in the Americas regarding transparency and access to information related to state surveillance activities. The Special Rapporteur notes that these transparency deficits are evidenced by multiple cases of illegal espionage against human rights defenders, journalists, magistrates, and political opponents that have occurred in various countries of the hemisphere, even under democratically-elected governments.[312]

192. The SRFOE has also addressed these issues in its prior thematic report on Access to Information and National Security (2020). The report documented persistent challenges in transparency and access to information about state surveillance in the Americas, noting how security classifications often prevent accountability. It highlighted how lack of transparency around surveillance activities acts as a barrier to ensuring judicial oversight and proportionality requirements.[313]

193. Moreover, as the UN Special Rapporteur on freedom of expression has explained, "While it is common for States to seek to justify restrictions, especially targeted surveillance, on the bases of national security, the Special Rapporteur has found that this rationale should be limited in

[307] Information submitted by Amnesty International, Americas Regional Office, in response to the public consultation by the IACHR Office Special Rapporteur for Freedom of Expression, August 2024, p. 5 ("The lack of transparency around the use of spyware, however, makes it difficult for victims to obtain information or to seek accountability. In line with international human rights law standards applied in the context of technology use, States have a duty to create an accountability framework that provides equal and effective access to justice for all; establishes mechanisms for effective, prompt, thorough and impartial investigations, including access to relevant information; and offers adequate, prompt and effective reparations including non-repetition guarantees").

[308] IACHR, Background and Interpretation of the Declaration of Principles, 2000.

[309] Organization of American States (OAS), Inter-American Model Law 2.0 on Access to Public Information, 2020.

[310] Open Society Justice Initiative, The Global Principles on National Security and the Right to Information (The Tshwane Principles).

[311] CIDH, Relatoría Especial para la Libertad de Expresión, Derecho a la información y seguridad nacional, OEA/Ser.L/V/II CIDH/RELE/INF.24/20, julio de 2020, párr. 56 y siguientes.

[312] CIDH, Relatoría Especial para la Libertad de Expresión, Derecho a la información y seguridad nacional, OEA/Ser.L/V/II CIDH/RELE/INF.24/20, julio de 2020, párr. 56 y siguientes.

[313] IACHR, Office of the Special Rapporteur for Freedom of Expression, Report Derecho a la información y seguridad nacional, OEA/Ser.L/V/II CIDH/RELE/INF.24/20, July 2020, para. 64 et seq.

application to situations in which the interest of the whole nation is at stake, which would thereby exclude restrictions in the sole interest of a Government, regime or power group."[314] Invocation of national security does not provide the state *carte blanche* to conduct surveillance operations against regime critics.

194. Obstacles to access to public information and the lack of transparency surrounding state surveillance activities often operate as barriers that prevent accountability regarding their legitimate use, which should follow requirements of prior judicial authorization and be strictly necessary and proportional to the legitimate ends sought to be protected by the state.[315]

195. The SRFOE reaffirms that the right to access public information—as encompassed within Article 13 of the American Convention—protects the right of every person to access information held by public authorities, including information related to national security. Access to such information may be restricted exceptionally, based on clear and precise exceptions established by law, provided that these are necessary in a democratic society to safeguard legitimate national security interests.

196. In the assessment of this Office, national security interests are favored in practice when society is properly informed about state activities, including those carried out to safeguard national security. In this sense, no information can be excluded a priori from public oversight simply because it is held by a national security agency or relates to national security matters, or because it fits into a particular category of information.[316]

197. Domestic law must be "accessible, unambiguous and drafted in a narrow and precise manner to allow people to understand what information can be classified, what should be disclosed, and what acts relating to information may be subject to sanctions."[317] In addition, national legislation must "define exactly the concept of national security and clearly specify the criteria to be used to determine whether certain information can or cannot be declared secret, in order to prevent abuse of the 'secret' classification to avoid disclosure of information that is in the public interest."[318]

198. In this regard, the Special Rapporteurship highlights that states must clearly and precisely define legitimate national security interests in legislation, observing that the concept of national security must be interpreted through a democratic lens. The regulation of exceptions must follow the principle of maximum disclosure, with such exceptions being truly exceptional. Moreover, when defining exceptions, they must be subject in each specific case to a time limit and condition, so that it is clear in the legislation that information cannot be removed from public knowledge indefinitely.[319]

199. As was recognized by the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism – a topic that implicates many of the same

---

[314] UN, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Surveillance and human rights, A/HRC/41/35, May 28, 2019, para. 24(c).

[315] CIDH, Relatoría Especial para la Libertad de Expresión, Derecho a la información y seguridad nacional, OEA/Ser.L/V/II CIDH/RELE/INF.24/20, julio de 2020, párr. 56 y siguientes.

[316] CIDH, Relatoría Especial para la Libertad de Expresión, Derecho a la información y seguridad nacional, OEA/Ser.L/V/II CIDH/RELE/INF.24/20, julio de 2020, párr. 87.

[317] Open Society Foundations/Open Society Justice Initiative, Principios globales sobre seguridad nacional y el derecho a la información [Principios de Tshwane], 12 de junio de 2013, Principio 3.A.

[318] Open Society Foundations/Open Society Justice Initiative, Principios globales sobre seguridad nacional y el derecho a la información [Principios de Tshwane], 12 de junio de 2013, Principio 2.C.

[319] CIDH, Relatoría Especial para la Libertad de Expresión, Derecho a la información y seguridad nacional, OEA/Ser.L/V/II CIDH/RELE/INF.24/20, julio de 2020, párr. 85.

national security considerations as use of surveillance technologies – "effective counter-terrorism measures and the protection of human rights are not conflicting, but rather complementary and mutually reinforcing goals. This also reflects the flexibility of human rights law. Through the careful application of human rights law it is possible to respond effectively to the challenges involved in the countering of terrorism while complying with human rights. *There is no need in this process for a balancing between human rights and security, as the proper balance can and must be found within human rights law itself. Law is the balance, not a weight to be measured*" (emphasis added).[320] Similarly, enhanced transparency concerning surveillance practices is not something for states to shy away from; rather, it should be embraced as a means of ensuring compliance with international human rights law, as well as improving the effectiveness, efficiency, and public understanding of surveillance operations.

200. In line with international best practices, the Tshwane Principles provide essential guidance for states to implement necessary measures when protecting national security in a manner consistent with a democratic society.[321] Particularly relevant is Principle 9, which sets forth a limited list of information categories with respect to which, if strictly necessary to protect legitimate national security interests, authorities could temporarily restrict access, provided such restrictions comply with all other Principles.[322]

201. States must develop clear legal parameters that limit the scope of secrecy claims in surveillance-related proceedings. Drawing from international best practices, including the Tshwane Principles, states should adopt legislation ensuring that information regarding human rights violations through surveillance cannot be withheld on national security grounds when such withholding would prevent accountability or deprive victims of effective remedy.[323] This requires establishing oversight bodies that can review classification decisions and ensuring effective judicial remedies for those seeking access to information.[324]

202. While transparency and access to information constitute essential foundations for accountability, effective protection against surveillance abuses requires comprehensive remedy mechanisms that address the full spectrum of harms caused by unlawful surveillance practices. In the view of the Special Rapporteur, legislation and other means of access to remedy have failed to keep pace with the modernization of state surveillance apparatuses. Proactive, practical, tailored measures are required to establish legal remedies for surveillance abuses. States must design such measures to provide predictability, transparency, and assurances of non-repetition, in order to prevent ongoing harm and further erosion of public trust.

203. As discussed throughout this report, at a minimum, access to remedy requires states to address issues of jurisdiction, evidentiary burdens, secrecy and confidentiality parameters, judicial independence, and notification to individuals impacted by surveillance operations. Access to remedy must also account for the wide range of harm experienced by those who suffer surveillance abuses, including psychosocial impacts and intersectional and gender-based harms.

---

[320] UN, General Assembly, Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, A/HRC/16/51, December 22, 2010, para. 12.

[321] Open Society Foundations/Open Society Justice Initiative, Principios globales sobre seguridad nacional y el derecho a la información [Principios de Tshwane], 12 de junio de 2013, Principio 2.C.

[322] Open Society Foundations/Open Society Justice Initiative, Principios globales sobre seguridad nacional y el derecho a la información [Principios de Tshwane], 12 de junio de 2013, Principio 9.

[323] See Open Society, The Global Principles on National Security and the Right to Information (The Tshwane Principles), June 12, 2013, Principle 10.

[324] IACHR, Office of the Special Rapporteur for Freedom of Expression, Report Derecho a la información y seguridad nacional, OEA/Ser.L/V/II CIDH/RELE/INF.24/20, July 2020, para. 87.

204. States must address the complex jurisdictional challenges inherent in digital surveillance operations. The transnational nature of surveillance technologies, including spyware deployed across borders and surveillance infrastructure operated by foreign companies, creates jurisdictional gaps that often leave victims without recourse. This Office observes that states should establish clear legal frameworks recognizing jurisdiction in cases where their nationals or residents are targeted by foreign surveillance operations, while also ensuring that their own surveillance activities comply with international human rights law regardless of where they occur[325].

205. In addition, the SRFOE notes that traditional evidentiary standards create insurmountable barriers for surveillance victims seeking remedy. As documented throughout this report, individuals subjected to surveillance often cannot obtain evidence of such targeting, confronting a state of secrecy that systematically prevents accountability. In the view of this Office, states must fundamentally reform evidentiary standards in surveillance-related cases. This includes shifting the burden of proof when plaintiffs provide credible indicators of surveillance targeting, such as technical forensic evidence or patterns of suspicious digital activity. Once a claimant establishes a *prima facie* case of surveillance targeting through available technical evidence, the burden should shift to the state to demonstrate compliance with legal authorization procedures and human rights standards.

206. Moreover, states should establish specialized evidentiary procedures that account for the technical complexity of digital surveillance. This includes creating mechanisms for independent technical expertise, protecting the integrity of forensic evidence and the ability of security researchers to engage in forensic investigation, and ensuring that victims have access to qualified technical assistance in building their cases.

[325] The jurisdictional complexities of transnational surveillance were identified as a key area requiring further development during the peer review consultations conducted with specialized organizations and experts for this report.

III. PROGRESS AND GOOD PRACTICE

207. While the international community has made significant progress in documenting surveillance abuses and recognizing the human rights impacts of surveillance practices, much work remains to effectuate reform. Challenges include continued and increasing demand for surveillance technologies by state entities, fragmentation among states in policy approaches, and lack of internal coherence within governments regarding use of commercial surveillance tools.[326] Export control reforms, in particular, have suffered from uneven application among individual states, competing policy priorities, and workarounds by the commercial market such as relocation in order to continue supplying their products and services.[327] Even so, a few developments stand out as concrete initiatives to promote accountability and provide the building blocks for further progress.

208. Following extensive investigations and reporting of spyware abuses, including the work of the Pegasus Project in 2021,[328] the European Parliament established its PEGA committee in March 2022 to "investigate alleged contraventions, or maladministration in the implementation, of Union law as regards the use of the Pegasus and equivalent surveillance spyware."[329] The inquiry consolidated understanding of the risks to human rights, democratic principles, and security presented by commercial spyware,[330] and produced recommendations for action and reform.[331]

209. The limits of such inquiries are apparent, however, in the varied progress on PEGA recommendations of EU states implicated in spyware scandals.[332] One positive example has been that of Poland: following 2023 elections that replaced the ruling party alleged to have abused spyware, the Polish parliament launched a probe of the abuses, working to bring transparency to the scope of misuse and accountability of those officials involved.[333]

210. The government of Costa Rica,[334] as well as a wide range of civil society groups, independent experts, and UN special rapporteurs, have called for a moratorium on the sale, transfer, and use of spyware, until such time as effective human rights safeguards are put in place regarding such practices to ensure legitimate use.[335]

---

[326] See. e.g., Carnegie Endowment for International Peace, Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses, March 14, 2023; International Security Programme, Principles for state approaches to commercial cyber intrusion capabilities, Octubre 2024, pp. 21-22

[327] Sipri, Export controls and cyber-surveillance tools: Five suggestions for the Summit for Democracy | March 8, 2024; Lawfare, Export Control is Not a Magic Bullet for Cyber Mercenaries, March 22, 2023.

[328] Forbidden Stories, The Pegasus Project: A worldwide collaboration to counter a global crime, July 18, 2021.

[329] European Parliament, decision: setting up a committee of inquiry to investigate the use of the Pegasus and equivalent surveillance spyware, March 10, 2022.

[330] See Think Tank, The existing legal framework in EU Member States for the acquisition and use of Pegasus and equivalent surveillance spyware, December 5, 2022; European Parliament, REPORT of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware, May 22, 2023.

[331] European Parliament, Investigation of the use of Pegasus and equivalent surveillance spyware (Recommendation), June 15, 2023.

[332] See European Parliament, Setting spyware standards after Europe's spying scandal, November 2024.

[333] CyberScoop, Inside Poland's groundbreaking effort to reckon with spyware abuses, May 15, 2024. The Record from Recorded Future News, Former Polish justice minister arrested in sprawling spyware probe, January 31, 2025.

[334] Access Now, Costa Rica: first country to call for a moratorium on spyware technology, April 13, 2022.

[335] UN, General Assembly, Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/41/35, May 28, 2019, para. 2; Amnesty International, Joint open letter by civil society organizations and independent experts calling on states to implement an immediate moratorium on the sale, transfer and use of surveillance technology, July 27, 2021; Cyber Peace Institute, Renewed Call for Moratorium on Sale and Use of Spyware, May 25, 2022; OACNUDH, Special Procedures, Spyware scandal: UN experts call for moratorium on sale of 'life threatening' surveillance tech, August 12, 2021.

211. With the increasing recognition of the risks presented by surveillance technologies and the need for a coordinated approach to regulation, a number of states have worked multilaterally to constrain the abuse and proliferation of surveillance technologies, and shape behavior within the broader surveillance market. The U.S. issued a Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware,[336] laying out a series of commitments undertaken by signatory states to address the threats presented by spyware to human rights and national security. Such commitments include "establish[ing] robust guardrails and procedures to ensure that any commercial spyware use by our governments is consistent with respect for universal human rights, the rule of law, and civil rights and civil liberties;" and "preventing the export of software, technology, and equipment to end-users who are likely to use them for malicious cyber activity."[337] An additional 22 countries have joined the statement; in the Americas, signatories are the U.S., Canada, and Costa Rica.[338]

212. The U.S., Canada, Ecuador, and an additional 21 countries[339] signed onto the Code of Conduct for Enhancing Export Controls of Goods and Technology That Could be Misused and Lead to Serious Violations or Abuses of Human Rights in 2023.[340] The Code of Conduct reflects commitments to, inter alia, "control the export of dual-use goods or technologies to end-users that could misuse them for the purposes of serious violations or abuses of human rights," and promote industry cooperation with the UN Guiding Principles on Business and Human Rights.[341]

213. The Freedom Online Coalition adopted Guiding Principles on Government Use of Surveillance Technologies in 2023, on the basis of consensus among its 36 member states.[342] Enumerated principles are appropriate legal protections; nondiscrimination; oversight and accountability; transparency; limitations on data scope and collection; secure post-acquisition data handling; respect for human rights, including privacy; integrity; training. The scope of the principles, however, is limited to three surveillance technologies of concern: Internet controls; advanced video surveillance that incorporates AI-driven identification and monitoring tools; and big data analytic controls.[343] Signatories to the Guiding Principles include the member states of the Freedom Online Coalition, such as Argentina, Canada, Chile, Colombia, Costa Rica, Mexico, and the U.S.,[344] as well as Ecuador.[345]

214. The U.S. Department of Commerce has added surveillance technology companies known to provide technology or services utilized in surveillance abuses to the Bureau of Industry and Security Entity List, which identifies entities of national security or foreign policy concern to which export

[336] U.S. Department of State, Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware, September 22, 2024.
[337] U.S. Department of State, Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware, September 22, 2024.
[338] U.S. Department of State, Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware, September 22, 2024.
[339] United States, Bureau of Industry and Security (BIS), Biden Administration and International Partners Release Export Controls and Human Rights Initiative Code of Conduct, March 30, 2023.
[340] United States, Department of State, Code of Conduct for Enhancing Export Controls of Goods and Technology That Could be Misused and Lead to Serious Violations or Abuses of Human Rights, March 30, 2023.
[341] United States, Department of State, Code of Conduct for Enhancing Export Controls of Goods and Technology That Could be Misused and Lead to Serious Violations or Abuses of Human Rights, March 30, 2023.
[342] Freedom Online Coalition, Guiding Principles on Government Use of Surveillance Technologies, March 2023.
[343] Freedom Online Coalition, Guiding Principles on Government Use of Surveillance Technologies, March 2023.
[344] Freedom Online Coalition, members.
[345] International Center For Not For Profit Law, Guiding Principles on Government Use of Surveillance Technologies, March, 2023.

restrictions apply.[346] The U.S. has also applied sanctions and visa restrictions against companies and individuals involved in such abuses.[347] Additional measures undertaken to further operationalize U.S. commitments on spyware included a 2023 executive order prohibiting use by the U.S. government of commercial spyware when "such use poses significant counterintelligence or security risks to the United States Government" or "the commercial spyware poses significant risks of improper use by a foreign government or foreign person," which includes threats to human rights;[348] and a 2023 intelligence community directive limiting the activities of former intelligence community employees that could impact national security or human rights,[349] which reflects concerns raised around the practice of state intelligence personnel moving on from government employment to the lucrative commercial market for surveillance technologies.

215. The UK and France spearheaded the Pall Mall Process in 2024, a multistakeholder dialogue to address the proliferation and irresponsible use of cyber intrusion capabilities.[350] The Pall Mall Process Declaration identifies accountability, precision, oversight, and transparency as priorities for engagement.[351] The goal of the Pall Mall Process is to highlight policy options and undertake the development of guiding principles for states, industry participants, and other stakeholders regarding "the development, facilitation, purchase, and use" of commercial cyber intrusion capabilities.[352]

216. In parallel to these developments, multilateral efforts to enhance data protection and cyber resilience have the potential to significantly impact this field. The Special Rapporteur notes with particular interest the European Commission for Democracy through Law (Venice Commission) December 2024 report on "A Rule of Law and Human Rights Compliant Regulation of Spyware," which provides concrete guidance on minimum safeguards for intrusive surveillance measures.[353]

217. The Venice Commission's analysis is particularly relevant to the Americas context, as it identifies minimum safeguards concerning intrusive measures of targeted surveillance that are essential to preventing unlawful surveillance practices, that transcend regional boundaries and align with universal human rights principles. The Commission emphasizes that "having regard to the particularly high level of intrusiveness of spyware, in particular the fact that it can involve a combination of different intrusions into privacy," States should enact "specific and tailored legislation with a stricter scope *ratione personae*, *materiae* and *temporis vis-à-vis* other targeted surveillance measures."[354]

---

[346] U.S. Department of Commerce, Press Releases: Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities, November 3, 2021.

[347] Access Now, Bigger, bolder: U.S. slaps sanctions on spyware company and executives, March 7, 2024; U.S. Department of the Treasury, Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium, March 5, 2024; The Verge, Spyware dealers could face visa restrictions, April 25, 2024.

[348] Federal Register, The Daily Journal of the United States Government, Prohibition on Use by the United States Government of Commercial Spyware That Poses Risks to National Security, March 27, 2023;

[349] United State of America, Office of the Director of National Intelligence, (U) Requirements for Certain Employment Activities by Former Intelligence Community Employees.

[350] GOV.UK, Pall Mall Process on proliferation and irresponsible use of commercial cyber intrusion capabilities: UK and France joint communiqué, February 7, 2024.

[351] Pall Mall Process, THE PALL MALL PROCESS: Tackling the Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities, February 6, 2024.

[352] Pall Mall Process, Consultation On Good Practices.

[353] Council of Europe, European Commission for Democracy through Law (Venice Commission), "Report on a Rule of Law and Human Rights Compliant Regulation of Spyware," CDL-AD(2024)043, adopted at the 141st Plenary Session, December 6-7, 2024.

[354] Council of Europe, European Commission for Democracy through Law (Venice Commission), "Report on a Rule of Law and Human Rights Compliant Regulation of Spyware," CDL-AD(2024)043, adopted at the 141st Plenary Session, December 6-7, 2024, para. 82.

218. Key among the Venice Commission's minimum safeguards are requirements that all significant provisions regulating spyware use must be set out in primary legislation; requesting authorities must demonstrate that information sought could not be obtained by less intrusive means; there must be well-regulated ex-ante authorization procedures before a court or independent body; effective external independent oversight institutions must oversee the surveillance process; and persons under surveillance must be notified subsequently to enable monitoring and challenging of the measures.

219. Of particular relevance is the Commission's emphasis that legislation should narrowly define possible targets and "provide that certain categories of persons whose interactions may be protected by professional privilege as well as journalists are in principle excluded," reflecting recognition of the special protection required for those engaged in activities essential to democratic discourse.[355]

220. The interplay between surveillance regulation, data protection, and cyber resilience merits additional study and engagement. As the Venice Commission noted, if kept unregulated, spyware "might turn into a 24-hour surveillance device, gaining complete access to all sensors and information on the personal device," transforming it into "a surveillance weapon that could be used to curtail human rights, censor and criminalise criticism and dissent and harass (if not suppress) journalists, human rights activists, political opponents, or repress civil society organisations."[356] This analysis reinforces the urgency of implementing comprehensive legal and technical safeguards across all three domains in the Americas.

221. International initiatives to address surveillance abuses and regulate the surveillance market have reached a critical stage, informed by an enormous amount of research, investigation, analysis, and engagement. Stakeholders in the Americas can build on these initiatives as they work to ensure surveillance practices comply with international human rights law, and prevent human rights abuses.

[355] Council of Europe, European Commission for Democracy through Law (Venice Commission), "Report on a Rule of Law and Human Rights Compliant Regulation of Spyware," CDL-AD(2024)043, adopted at the 141st Plenary Session, December 6-7, 2024, para. 96.

[356] Council of Europe, European Commission for Democracy through Law (Venice Commission), "Report on a Rule of Law and Human Rights Compliant Regulation of Spyware," CDL-AD(2024)043, adopted at the 141st Plenary Session, December 6-7, 2024, para. 135.

IV. LEGITIMACY IN THE SURVEILLED WORLD: DISTINGUISHING LEGITIMATE FROM INDISCRIMINATE USE OF SURVEILLANCE TECHNOLOGIES

222. The Special Rapporteur observes, based on the interviews, accumulated research and reporting, and years of multilateral engagement described within this report, that a persistent shortcoming in addressing the human rights impacts of surveillance is the reluctance of states and the private sector to scrutinize–and subject to public scrutiny–the concept of "legitimate use" of surveillance technologies. Multilateral discussion regarding surveillance has emphasized the 'legitimate use case' of intrusive surveillance tools, as state authorities as well as private companies and investors have sought to preserve their ability to participate in the digital surveillance market. In the view of the Special Rapporteur, however, legitimacy is, by its very nature, earned. A blanket proclamation of legitimacy by a state, without more, can satisfy neither the requirements of international human rights law nor critical public perception.

223. It bears repeating that international human rights law considers state use of surveillance curtailing the rights to freedom of expression and privacy to be an *exception* within the legal framework, not a right: it is only permissible when in furtherance of a legitimate aim recognized under human rights law (i.e., respect of the rights or reputations of others, or the protection of national security or of public order), and in conformity with the principles of legality, necessity and proportionality. Restrictions on the right to freedom of expression "may not put in jeopardy the right itself… [T]he relation between right and restriction and between norm and exception must not be reversed."[357]

224. Emphasizing states' ability to engage in surveillance as opposed to the clear limitations on permissible surveillance activity runs the risk of further normalizing surveillance and encouraging disregard for international human rights law. The exception cannot outweigh the right, and legitimacy of use cannot be presumed. Indeed, the track record on use of surveillance technologies in the Americas suggests that many states engage in indiscriminate deployment of particular surveillance tools, rather than careful assessment of compliance with robust legal frameworks.

225. The ironclad secrecy associated with state use of surveillance tools, coupled with a predictable and nearly universal lack of remedy for those who have been illegally targeted, require a reckoning with the application of international human rights law at large in the arena of digital surveillance by states. Certainly international human rights law, as embodied in the American Convention and the ICCPR, did not contemplate an exception to fundamental human rights that would enable a state, facilitated by the private sector, to surveil human rights defenders, journalists, regime critics, or other political opponents with impunity. Yet that is precisely the current reality within many states in the Americas.

226. What is missing in the practical application of international human rights law to modern state surveillance are reliable mechanisms to assess whether the state is *meeting* the well-established legal requirements of legitimate aim, necessity and proportionality in its surveillance activities. Most forms of digital surveillance are invisible to the public, and state invocation of national security, state secrets and the like as a defense to revealing information about surveillance practices further prevents opportunity for assessment. Yet that inability to assess the state in the arena of surveillance, with an eye to application of the principles of human rights law, is a glaring loophole that has opened the door for severe human rights abuses.

[357] UN, Human Rights Committee, General comment No. 34: Article 19: Freedoms of opinion and expression, CCPR/C/GC/34, 12 September 2011, para. 21.

227. Accordingly, it is essential to address the implicit parameters of international human rights law that allow for such assessment in order to determine the legitimacy of surveillance use.

A. The Inter-American Court's approach to surveillance

228. The decision of the Court in the *Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia* provides essential guidance in this endeavor. The Court noted precisely this need to

> identify the requirements and controls to which intelligence activities must be subject in order to affirm their validity and legitimacy in a democratic system and, consequently, their compatibility with human rights and the American Convention. This is of great importance not only because of the imminent friction that arises between intelligence activities and the rights of the person, but also because normally this type of operation, in order to ensure the effective performance of its tasks, is carried out in a reserved or secret manner, without the knowledge of the general population and without the consent of those who could be directly affected, increasing the risk of an abusive or arbitrary exercise of public power.[358]

229. The Court identified a set of criteria essential to evaluating legitimacy of state surveillance operations. These criteria are addressed below.

1. Fulfillment of the international human rights law requirements of legality, legitimate aim, suitability, necessity, and proportionality

230. State surveillance operations must always meet the test laid out by international human rights law for permissible limitations on the rights to freedom of expression and to privacy.[359]

231. The principle of legality requires that "the legal framework define intelligence activities, the purposes to be pursued through them, and the powers of the competent bodies and authorities. In this regard, it is essential that a law precisely regulate such aspects, the content of which must be accessible to the general public."[360] Accordingly, the legal framework governing the use of surveillance technologies must itself be public. It must specify the authorities imbued with such powers, the scope of and limitations upon such powers, and the criteria used in authorizing surveillance activities.

232. Use of surveillance technologies must be in pursuit of a legitimate aim, namely, the protection of national security; the maintenance of public order; the safeguarding of public health; or the

[358] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections, Merits, Reparations and Costs. October 18, 2023. Series C No. 506, para. 527.
[359] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections, Merits, Reparations and Costs. October 18, 2023. Series C No. 506, para. 521.
[360] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections, Merits, Reparations and Costs. October 18, 2023. Series C No. 506, para. 528.

protection of human rights.[361] While states have invoked such concepts broadly to cover a wide range of activity, the Court clarified:

> [T]he legitimate purposes identified above prohibit any intelligence activity with discriminatory purposes based on race, color, sex, language, religion, political or other opinions, national or social origin, economic position, birth or any other social condition (Article 1.1 of the American Convention). The above determines that it is prohibited for the functions of intelligence agencies to be exercised with the objective of promoting, benefiting or affecting a certain activity, person or group due to their ideology or political opinion, religious belief, social condition, economic position or for any other reason.[362]

It is therefore not a legitimate aim of surveillance to target individuals or groups on the basis of their identity or dissenting political viewpoints.

233. Surveillance activities must comply with the requirements of suitability, necessity and proportionality.[363] As the Court specified, the competent authorities must carry out a "proportionality judgment" in authorizing or implementing specific surveillance activities, which requires,

> in addition to the legal provision of said activities and the achievement of a legitimate end, the following: a) that the intelligence actions or operations undertaken are suitable or adequate to fulfill the legitimate end pursued; (b) that intelligence activities in general, and the actions or methods employed in particular, are necessary in the sense that they are absolutely indispensable for achieving the desired end and that there is no less burdensome measure, due to its interference with the right to privacy or any other right that may be affected, among all those other actions or strategies that are equally suited to achieving the proposed objective, and (c) that intelligence actions are strictly proportional, such that the sacrifice inherent in restricting the right involved does not become exaggerated or disproportionate compared to the advantages obtained through such restriction and the fulfillment of the intended purpose.[364]

234. Such judgment requires careful individualized assessment and guards against arbitrary and indiscriminate use.

2. A robust domestic system for control of the use of surveillance technologies

235. The Court highlights that compliance with human rights law fundamentally requires domestic legislation to provide "'a well-defined and comprehensive system to authorize, monitor and supervise' intelligence activities in specific situations."[365] An effective domestic system of control

[361] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections, Merits, Reparations and Costs. October 18, 2023. Series C No. 506, para. 531.
[362] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections, Merits, Reparations and Costs. October 18, 2023. Series C No. 506, para. 535.
[363] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections, Merits, Reparations and Costs. October 18, 2023. Series C No. 506, para. 536.
[364] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections, Merits, Reparations and Costs. October 18, 2023. Series C No. 506, para. 537.
[365] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections, Merits, Reparations and Costs. October 18, 2023. Series C No. 506, para. 538.

for surveillance operations is crucial to reigning in surveillance abuses and ensuring that such operations meet the requirements of international human rights law.

236. Essential components of a comprehensive system of control include legislation that defines surveillance techniques and objectives, "classes of persons and activities in respect of which obtaining and gathering information is permitted," necessary degree of suspicion, and time periods within which surveillance is permitted.[366] The Court highlighted the importance of robust record-keeping as well, including registration of all stages of intelligence operations, responsible personnel, access and alteration histories, processing techniques, retention periods, and the legal bases on which operations are carried out.[367]

237. A robust domestic system of control requires effective *ex ante* oversight, the foremost example of which is judicial authorization for intrusive surveillance operations. The Court found it "essential that judicial authorities be responsible for authorizing 'invasive measures for gathering information,' such as the interception of communications by telephone, correspondence or email, among other information and communications technology tools, or searches of homes, workplaces or other private premises."[368] Judicial authorities must undertake the requisite proportionality assessments, and determine the admissibility of material obtained through surveillance operations.[369] Moreover, states must adequately equip judicial authorities to handle surveillance authorizations in myriad contexts, including situations of urgency. The judicial authorization process can serve as a fundamental check on surveillance overreach when judicial authorities operate with independence and appropriate resources.

238. Additionally, the Court recognized that "it is essential to limit intelligence actions with respect to certain categories of persons, particularly journalists, in order to safeguard the confidentiality of their sources, and lawyers, in order to guarantee the confidentiality of the communications they maintain with their clients and clients within the framework of their professional relationship."[370] A robust system for surveillance control should identify those groups of people that have been subjected to surveillance abuses in the past, and to whom presumptions of protection should apply in furtherance of human rights and public policy objectives.

239. Effective domestic systems of surveillance control require the marshalling of political will, and must be built over time, on the basis of support and shared learning among states. The Special Rapporteur notes in particular that legitimacy requires more than development of the domestic legal framework itself; it depends on faithful adherence to and implementation of the law, which requires adequate resources and trained, well-tasked personnel. State authorities must provide due consideration in budgetary and staffing decisions to the matter of surveillance compliance.

3. An independent civilian oversight authority

[366] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections, Merits, Reparations and Costs. October 18, 2023. Series C No. 506, para. 539.
[367] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections, Merits, Reparations and Costs. October 18, 2023. Series C No. 506, paras. 540-541.
[368] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections, Merits, Reparations and Costs. October 18, 2023. Series C No. 506, para. 542.
[369] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections, Merits, Reparations and Costs. October 18, 2023. Series C No. 506, paras. 562, 547.
[370] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections, Merits, Reparations and Costs. October 18, 2023. Series C No. 506, para. 555.

240. The Court emphasized the need for an independent civilian authority to provide an additional lawyer of oversight to state surveillance operations, empowered with access to budget and other detailed information regarding those operations. It states:

> With regard to the supervision of intelligence activities, it is necessary that the legal framework establish, without prejudice to judicial control over specific measures or actions in specific situations, *a civilian institution independent of the intelligence services and the Executive Branch*, of a parliamentary, administrative or jurisdictional nature, which, in addition to having the technical knowledge on the subject, must be *endowed with the powers to exercise its functions, including direct and complete access to the information and data essential to fulfill its mission*. The mandate of this civilian oversight institution must cover oversight of the following aspects: a) the compliance by the intelligence services with the legal provisions governing their actions and with human rights instruments; b) the efficiency and effectiveness of their activities, evaluating their performance; c) their financial and budgetary situation, and the administration of their funds; and d) their administrative methods and practices (emphasis added).[371]

241. As the Court made clear, proper civilian oversight is only possible on the basis of fit-for-purpose transparency mechanisms. While states have a reasonable need to maintain secrecy around some aspects of their surveillance operations, that secrecy is not unqualified. Progress requires a good faith effort by all stakeholders to address transparency in the context of state surveillance.

242. The lack of transparency around surveillance operations is a longstanding issue on which much work already exists. For example, the Global Principles on National Security and the Right to Information (the Tshwane Principles) provide guidance on ensuring public access to information in the context of national security.[372]As the Tshwane Principles state:

> (1) There is an overriding public interest in disclosure of information regarding gross violations of human rights . . . .. Such information may not be withheld on national security grounds in any circumstances.
> (2) Information regarding other violations of human rights or humanitarian law is subject to a high presumption of disclosure, and in any event may not be withheld on national security grounds in a manner that would prevent accountability for the violations or deprive a victim of access to an effective remedy.[373]

243. In order to effectuate public oversight, some form of public reporting is essential, including at a minimum: disclosure of government contracts and the use of public funds for surveillance-related equipment and services; registries of surveillance vendors and disclosures regarding the contractor pool; disclosure of the tools purchased by the state and their specifications; disclosures regarding agencies authorized to engage in surveillance; and statistics regarding use. As R3D has pointed out, "Even when Pegasus use has been exposed, it continues to be used… even against the same people. Even when the technical capabilities were already public, that didn't stop the tool from being efficient. We need to push back on the effective secrecy of the tools and what the state has. The

[371] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections, Merits, Reparations and Costs. October 18, 2023. Series C No. 506, para. 564.

[372] Open Society, The Global Principles on National Security and the Right to Information (The Tshwane Principles), June 12, 2013.

[373] Open Society, The Global Principles on National Security and the Right to Information (The Tshwane Principles), June 12, 2013, Principle 10.

public should be able to know this, and engage in democratic discourse and debate about what tools are reasonable and acceptable in our societies."[374]

244. The very ubiquity of and widespread reliance upon advanced digital tools with law enforcement and intelligence applications weighs in favor of broad, systematic disclosure. While details in precise application may warrant secrecy, public dialogue around capabilities, vendors, authorized operators, and statistics on deployment will promote healthy and better processes for procurement and use, as well as better understanding within society of security of the digital ecosystem. Moreover, it will promote transparency in the use of public funds.

245. Efforts to establish an independent civilian oversight authority should also include consideration of the role of vulnerabilities equities processes (VEPs). VEPs are governmental processes through which a state decides whether to disclose newly discovered software vulnerabilities with affected companies for patching, or to withhold them for operational purposes. These include law enforcement investigations, intelligence collection, and offensive cyber operations. This decision-making process is critical because the same software vulnerabilities that enable legitimate surveillance operations can also be exploited by malicious actors to compromise the security of the broader digital ecosystem.[375] In this regard, genuine oversight necessarily requires the participation of independent, expert representation of the public interest in VEPs, while maintaining essential confidentiality parameters.[376]

4. A mechanism for remedy and reparation in the event of surveillance abuse

246. As discussed earlier in this report, the impunity associated with surveillance abuses is a key impediment to human rights progress. The antidote to such impunity is genuine access to remedy and reparation for those who have experienced surveillance abuse. As the Court observed in *CAJAR,* "At the international level, there is also a requirement to provide mechanisms so that those who consider themselves affected by arbitrary intelligence activities can obtain effective reparation, including compensation for the damages caused." Such mechanism "must correspond, in the last instance of decision, to a simple, rapid and effective recourse before the courts of justice, whose decisions must be fully complied with and executed."[377]

247. States are obligated to create a path for redress, and companies have a responsibility to provide remedy, to those who have experienced surveillance abuses. Yet broad notions of national security and secrecy, combined with the transnational and opaque nature of surveillance infrastructure and operations, have largely prevented meaningful remedy to those impacted by surveillance.

248. Notably, the *CAJAR* parameters enumerated above are contemplated in similar fashion by the principles of the Pall Mall Process Declaration (oversight, transparency, accountability, precision); the Guiding Principles on Government Use of Surveillance Technologies; and the Necessary and

[374] Interview with R3D, August 23, 2024.

[375] The Mozilla Blog, The Vulnerabilities Equities Process, What we know and what we'd like to see, 2017; Harvard Kennedy School, Belfer Center for Science and International Affairs, Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process, June 2016.

[376] See, e.g., Lindsey Polley, To Disclose, or Not to Disclose, That Is the Question: A Methods-Based Approach for Examining & Improving the US Government's Vulnerabilities Equities Process, Pardee RAND Graduate School, March 2022; Daniel Pereira, "Will Expansion of the Vulnerabilities Equities Process (VEP) Strengthen National Security and Coalition Collaboration?", OODALoop, 12 October 2022.

[377] IACtHR. Case Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia. Preliminary Objections Merits, Reparations and Costs. October 18, 2023. Series C No. 506, para. 565.

Proportionate Principles, suggesting a developing consensus on what elements are required to determine legitimacy in state use of surveillance technologies.

B. Guardrails around private sector participation in state surveillance

249. As years of research and reporting on surveillance abuses has demonstrated, participation of the private sector in state surveillance activities has resulted in the proliferation of advanced surveillance capabilities around the globe, exacerbated rights abuses, and stymied transparency and accountability efforts. Much work already exists analyzing the human rights implications of the commercial spyware industry and recommending essential reforms, including the efforts of civil society groups,[378] the UN Special Rapporteur on freedom of opinion and expression,[379] and the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism.[380] States have also recognized "the need for greater international action and multi-stakeholder consultation" regarding the market for cyber intrusion technologies through the Pall Mall Process.[381]

250. In the view of the Special Rapporteur, it is clear that enhanced guardrails around private sector participation in state surveillance operations are required and long overdue. Private sector participation has enormous potential to undermine those elements previously identified in this report as critical to legitimacy of surveillance operations, namely, compliance with international human rights law; control and oversight; transparency; and access to remedy. If the private sector is to engage responsibly in this space in line with the UN Guiding Principles on Business and Human Rights,[382] clear means for transparency and channels for accountability must exist in the relationship between states and the private sector entities supporting their surveillance operations.

251. This conclusion is reinforced when considering the exceptionally broad scope of the rights implicated by the use of digital surveillance technologies, as discussed throughout this report—including the principle of personal autonomy itself. Indeed, while the commercial market for surveillance technologies has become deeply entrenched in state security apparatuses, it is important to reflect on the legality of commercial involvement in state surveillance in the first instance. Depending on the capabilities at issue, the development and deployment of highly intrusive surveillance technologies may properly be considered an "inherently state function," that is, activity that should only be undertaken by state actors, pursuant to legal frameworks compliant with international human rights law.[383]

---

[378] See, e.g., Access Now, The Geneva Declaration on Targeted Surveillance and Human Rights, September 29, 2022.

[379] UN, General Assembly, Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/41/35, May 28, 2019.

[380] UN, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Fionnuala Ní Aoláin, Human rights implications of the development, use and transfer of new technologies in the context of counterterrorism and countering and preventing violent extremism, A/HRC/52/39, March 1, 2023; Special Rapporteur on the Promotion and Protection of Human Rights While Countering Terrorism, Professor Fionnuala Ní Aoláin, Statement on the Development, Use, and Transfer of Commercial Spyware; Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Position paper: Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach, April 2023; Just Security, Spyware Out of the Shadows: The Need for A New International Regulatory Approach, May 16, 2023.

[381] Pall Mall Process, Tackling the Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities, Lancaster House, London, 6 February, 2024.

[382] UN, Office of the High Commissioner for Human Rights, Guiding Principles on Business and Human Rights, UN, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, HR/PUB/11/04, 2011.

[383] As the UN Working Group on the use of mercenaries stated in the analogous context of regulation of private military and security companies (PMSCs), "inherently state functions" are functions that the state "cannot outsource or delegate to PMSCs under any circumstances. Among such functions are direct participation in hostilities, waging war and/or combat operations, taking prisoners, law-making, espionage, intelligence, knowledge transfer with military, security and policing application . . . ." UN, Report of the Working Group

252. Particularly with respect to spyware, which is based on the offensive exploitation of vulnerabilities in consumer-facing technologies, legitimacy flows from color of state use, raising questions about the propriety of development of intrusive offensive tools *outside* of any framework of state contract or control—including vulnerability equities processes where they exist.[384] When states rely on commercial spyware rather than channeling capabilities through proper VEPs, they abdicate essential responsibility for the cybersecurity and human rights implications of their surveillance activities. Under established VEP frameworks, states must assess whether exploiting a vulnerability serves sufficiently important purposes to justify leaving millions of devices potentially vulnerable. Commercial spyware companies face no such constraints and operate with financial incentives directly conflicting with broader cybersecurity and human rights interests. The sequence of state involvement and control matters, and in the case of the spyware market, the tool is effectively developed and supported at a supranational level, undermining prospects for accountability and oversight. Such activity should be subject to robust VEPs and the kinds of public transparency, debate, accountability, and oversight that private sector participation systematically erodes.

253. The Special Rapporteur emphasizes that not all participants in the surveillance market present equivalent risks or challenges for regulation. As documented in Section II.A. of this report, the market for surveillance technologies is ever evolving, and encompasses a wide range of tools, some of which were originally purposed for entirely different use cases. Yet the lack of transparency surrounding digital surveillance operations complicates development of a granular approach to regulation of the surveillance market. Distinctions must be drawn between companies providing multifunctional technologies that may have dual-use applications, those offering targeted surveillance capabilities with potential legitimate law enforcement applications, and entities developing what can only be characterized as tools with no legitimate use in light of the parameters of international human rights law.

254. This Office considers that certain categories of surveillance technologies, particularly those designed for mass data collection without individualized suspicion, or comprehensive device compromise capabilities that lack technical safeguards,[385] fall into a category of "no legitimate use" under international human rights law. Such tools are inherently incompatible with the principles of necessity and proportionality that govern permissible restrictions on human rights, as they enable surveillance far exceeding what could be justified for any legitimate law enforcement or national security purpose.

255. The Rapporteurship observes that companies developing and marketing such illegitimate surveillance capabilities cannot claim good faith compliance with international human rights standards. When technologies are designed to enable mass surveillance, comprehensive device takeover, or other capabilities that systematically exceed the bounds of proportionate state action, their very development and commercialization constitute complicity in foreseeable human rights violations.

---

on the use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination, A/65/325, August 25, 2010, at Annex, Art. 2. See also David Kaye and Sarah McKune, The Scourge of Commercial Spyware—and How to Stop It, Lawfare, August 25, 2023.

[384] See Asaf Lubin, *Selling Surveillance*, Ohio State Law Journal, at pp. 872-873.

[385] UN, Special Rapporteur on the Promotion and Protection of Human Rights While Countering Terrorism, Professor Fionnuala Ní Aoláin, Statement on the Development, Use, and Transfer of Commercial Spyware ("[S]pyware which fails to display certain inbuilt limitations and controls should never be allowed, and at a minimum those controls should include powers to limit the scope of digital intrusion, markers and 'kill switches' in cases of misuse, and an indelible, permanent, uneditable and auditable record of actions taken by spyware users so that compliance can properly be assessed after the fact.").

256. The Special Rapporteur also notes with particular concern the role of private equity firms, venture capital funds, and other investment entities in enabling and profiting from surveillance technologies that systematically violate human rights. The Office observes that financial sector involvement adds another layer of profit-driven interests that fundamentally conflict with human rights compliance and democratic accountability.

257. As documented in the case of NSO Group, private equity backing creates structural impediments to responsible business conduct even when human rights abuses become publicly evident.[386] The Rapporteurship emphasizes that when surveillance companies are confronted with evidence of their products' negative human rights impacts, financial obligations to investors may prevent meaningful course correction.

258. In light of these concerns, this Office asserts that investment companies providing funding for surveillance technologies must be held accountable for foreseeable human rights violations enabled by their portfolio companies. Under the UN Guiding Principles on Business and Human Rights, financial institutions have responsibilities to conduct human rights due diligence and avoid contributing to adverse human rights impacts through their business relationships.[387]

259. "Self-regulation" by surveillance companies is an unlikely solely solution, particularly given the magnitude of the human rights impacts of and the national security interests in this sector. As the UN Special Rapporteur on contemporary forms of racism noted in her report on racial discrimination and emerging digital technologies:

> From a human rights perspective, relying on companies to regulate themselves is a mistake, and an abdication of State responsibility. The incentives for corporations to meaningfully protect human rights (especially for marginalized groups, which are not commercially dominant) can stand in direct opposition to profit motives. When the stakes are high, fiduciary obligations to shareholders will tend to matter more than considerations concerning the dignity and human rights of groups that have no means of holding these corporations to account. Furthermore, even well-intentioned corporations are at risk of developing and applying ethical guidelines using a largely technological lens, as opposed to the broader society-wide, dignity-based lens of the human rights framework.[388]

260. The UN Special Rapporteur on counter-terrorism and human rights raised similar concerns about self-regulation by spyware companies, underscoring that

> [T]he human rights stakes are too high to leave the solution to this global human rights crisis in the hands of those whose business model relies upon the growth of the use of this technology internationally. . . . Self-regulation is particularly unsuitable for a high-risk technology that has a demonstrated history of abuses and emanates from a sector that is marked by its lack of transparency and disregard of international human rights law.[389]

---

[386] David Kaye and Sarah McKune, The Scourge of Commercial Spyware—and How to Stop It, Lawfare, August 25, 2023.

[387] Surveillance Technologies Accountability Project, Navigating the Surveillance Technology Ecosystem: A Human Rights Due Diligence Guide for Investors, March 2022; Amnesty International, Operating in the shadows: Investor risk from the private surveillance industry, October 2021.

[388] UN, Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, Racial discrimination and emerging digital technologies: a human rights analysis, A/HRC/44/57, June 18, 2020, para. 62.

[389] UN, Special Rapporteur on the Promotion and Protection of Human Rights While Countering Terrorism, Professor Fionnuala Ní Aoláin, Statement on the Development, Use, and Transfer of Commercial Spyware, at para. 11.

261. Private sector initiatives to comply with the UN Guiding Principles on Business and Human Rights in the surveillance space have indeed come up short,[390] as in many cases companies' fulfillment of their human rights responsibilities would undermine market access and deference to their state clients, contractual confidentiality commitments, the strategic ability to develop ever-more intrusive technologies to maintain a competitive edge, and returns on investment.

262. In the view of the Special Rapporteur, the path forward requires a dramatic overhaul of transparency in the commercial surveillance market; proactive integration by surveillance companies of a human rights pillar in all aspects of operation; and the creation and widespread adoption by states, in consultation with industry and civil society, of new channels for private sector accountability. The participation of states will indeed be essential to each of the aforementioned endeavors, to properly incentivize companies and eliminate barriers to substantive reform.[391]

263. The Special Rapporteur offers the following suggestions as a basis for discussion of guardrails around private sector participation in state surveillance, recognizing that such initiatives will require extensive multi-stakeholder dialogue, commitment, and effort to effectuate.

264. ***Transparency:*** The Special Rapporteur notes the need for systematic, comprehensive, and regularly updated mapping of participants in the surveillance industry, the capabilities it offers, and use of its products and services. This requires not only the extensive contributions that civil society has provided, but improved and consistent reporting by states of surveillance-related export statistics, procurement policies and contracts, and budget information. It also requires mandated reporting (e.g., on the basis of procurement requirements) by surveillance companies themselves regarding the extent of their participation in the market, and sufficiently detailed information about their products and services. In the Special Rapporteur's view, it is high time for states and companies to publicly disclose surveillance capabilities and contracts, and acknowledge state use of surveillance technologies at a meaningful level of detail, in order to facilitate essential public debate about the role and necessary limitations of such surveillance in democratic societies, and ensure compliance with international human rights law.

265. ***Human rights as an operational pillar:*** Given the enormous potential of surveillance technologies to negatively impact human rights, and documented state track records of surveillance abuse, it is incumbent upon participants in the surveillance industry to proactively embrace human rights as a fundamental pillar of operation in order to prevent, mitigate, and remediate adverse human rights impacts associated with their products and services. Beyond the essentials of human rights due diligence and impact assessments, surveillance companies should incorporate human rights perspectives and policies throughout their operations, for example: in the design, development, marketing, sale, and servicing of their technologies; by implementing technical licensing systems that bifurcate license activation between an operator and an oversight authority; in hiring, training, and review of personnel; through human rights-oriented audits and software lifecycle management; in developing and negotiating contracts; by engaging in robust transparency reporting; and by building robust operational-level grievance mechanisms that ensure the confidentiality of communications with impacted individuals and provide timely notification of investigation outcomes. The Special Rapporteur also endorses the proposals of the UN Special

[390] See, e.g., Access Now, Rights Groups: NSO Group continues to fail in human rights compliance, April 21, 2021; UN, Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, OL OTH 52/2019, October 18, 2019.

[391] As the UN Guiding Principles on Business and Human Rights provide, "In meeting their duty to protect, States should: . . . Ensure that other laws and policies governing the creation and ongoing operation of business enterprises, such as corporate law, do not constrain but enable business respect for human rights." Principle 3(b).

Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism for a set of minimum requirements applicable to spyware companies, including with respect to the technical features of their products such as data access controls, flagging systems and 'kill switches,' and audit capabilities.[392]

266. ***New channels for private sector accountability:*** The Special Rapporteur notes the significant impact of U.S. sanctions and visa restrictions against individuals and entities documented to have facilitated spyware abuses,[393] and encourages other states to enact similar penalties. States should also urgently explore new channels for private sector accountability, including through legislation establishing jurisdiction, evidentiary standards, and private causes of action specific to digital surveillance abuses; procurement restrictions tied to a company's human rights record and practices; and empowering independent state authorities or multilateral bodies to investigate, publicly report on, and provide redress to those impacted by digital surveillance abuses. The Special Rapporteur further considers that meaningful regulation of the surveillance sector requires extending accountability mechanisms to include investors, creditors, and other financial actors whose profit motives drive the development and proliferation of rights-violating surveillance technologies. This includes requirements for enhanced due diligence, public reporting on surveillance-related investments, restrictions on investment in companies providing illegitimate surveillance capabilities; and liability mechanisms for investors who fund companies engaged in systematic human rights violations.

267. States are at a crossroads in determining the future trajectory of the role of digital surveillance technologies in their societies. If they wish to restore public trust, and prevent a normalization of surveillance that undermines human rights and democracy, a modernized and well-resourced framework for "legitimate" surveillance – that is, transparent and accountable surveillance use compliant with international human rights law – is required.

268. The Special Rapporteur emphasizes that a framework for "legitimate" surveillance must address the fundamental incompatibility between profit-driven commercial surveillance markets and human rights compliance. This includes recognizing that certain surveillance technologies have no legitimate use, requiring that states develop intrusive surveillance capabilities as inherently state functions subject to robust oversight including VEP processes, and extending accountability to the financial actors whose investments enable rights-violating surveillance technologies.

269. The use of digital surveillance technologies is only properly characterized as "legitimate" if legally authorized state entities use those tools in a manner that meets the requirements of international human rights law, provides a minimum level of public transparency, is subject to effective control and oversight, and is demonstrably accountable. In the view of this Office, the current commercial spyware model undermines these requirements and must be replaced with fundamentally different approaches that prioritize democratic accountability over private profit.

[392] Fionnuala Ní Aoláin, Global regulation of the counter-terrorism spyware technology trade: scoping proposals for a human-rights compliant approach, April 2023, at pp. 92-93.

[393] Access Now, Bigger, bolder: U.S. slaps sanctions on spyware company and executives, March 7, 2024; U.S. Department of the Treasury, Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium, March 5, 2024; The Verge, Spyware dealers could face visa restrictions, April 25, 2024.

V. CONCLUSIONS AND RECOMMENDATIONS

270. The SRFOE concludes that digital surveillance technologies have become a systemic threat to human rights across the Americas, fundamentally altering the relationship between states and their citizens. The evidence presented in this report demonstrates that surveillance practices previously considered exceptional under international human rights law have become increasingly normalized, creating a permissive environment for continuous violations of fundamental rights.

271. Surveillance technologies documented in this report—from commercial spyware to facial recognition systems, geolocation tracking, and mass data collection—have been deployed across the region with insufficient legal frameworks, inadequate oversight mechanisms, and minimal transparency. This systematic deployment has created what can only be characterized as a surveillance apparatus that operates outside the bounds of international human rights law, fundamentally undermining the principles of necessity, proportionality, and legality that must govern any restriction on human rights.

272. The Special Rapporteurship observes with particular concern that surveillance targeting has followed patterns that reveal its purpose: the maintenance of power and the suppression of dissent. The targeting of journalists, human rights defenders, political opposition, lawyers, and civil society actors documented in different countries and elsewhere demonstrates that surveillance is being used not for legitimate law enforcement or national security purposes, but as a tool of political control and repression.

273. The testimonies collected by this Office reveal the profound and lasting impacts of surveillance on freedom of expression, creating chilling effects that extend far beyond the individuals directly targeted. The documented cases of journalists who have ceased investigating sensitive topics, sources who refuse to engage with media, and human rights defenders who have curtailed their activities demonstrate how surveillance operates as a form of indirect censorship prohibited by Article 13(3) of the American Convention on Human Rights.

274. The normalization of surveillance has coincided with broader processes of democratic erosion in the region, creating conditions conducive to authoritarian governance. When states can systematically monitor journalists, human rights defenders, political opponents, and civil society, the essential mechanisms of democratic accountability are fundamentally undermined. The result is not merely individual rights violations but the systematic erosion of democratic institutions and the rule of law.

275. The emergence of "algorithmic governance" and predictive surveillance systems documented in this report represents a qualitatively new threat to human dignity and personal autonomy. These systems transform citizenship itself into a surveillance relationship, where accessing rights and services becomes contingent upon submitting to comprehensive monitoring and profiling by state authorities.

276. The information presented in this report demonstrates the urgent need for comprehensive mechanisms to prevent surveillance abuses before they occur, detect them when they happen, provide effective remedies to those who have been harmed, and sanction those entities perpetrating or complicit in rights abuses. The systematic nature of surveillance violations across the region reveals fundamental gaps in legal frameworks, oversight mechanisms, and accountability systems that must be addressed holistically.

277. Prevention requires robust legal frameworks that clearly define the circumstances under which surveillance may be deployed, establish meaningful judicial authorization procedures, and create independent oversight mechanisms with real powers to monitor compliance. Detection demands transparency regarding surveillance capabilities and deployment, notification systems that inform individuals when they have been subjected to surveillance, and technical assistance for civil society organizations to identify and document abuses.

278. Perhaps the most alarming finding of this report is the impunity that characterizes surveillance abuses across the region. Despite extensive documentation of illegal surveillance operations, no state in the Americas has successfully prosecuted those responsible for surveillance abuses or provided meaningful remedy to victims. This systematic failure of accountability mechanisms has created a permissive environment that encourages continued violations and demonstrates to both state and private sector actors that surveillance abuses will face no consequences.

279. The Special Rapporteurship concludes that the current state of impunity for surveillance abuses could constitute a violation of the right to effective remedy enshrined in Article 25 of the American Convention on Human Rights. The failure of states to investigate surveillance abuses, provide information to victims about the scope of surveillance targeting, or implement guarantees of non-repetition creates what can only be characterized as a continuous violation of rights that persists as long as victims remain without truth, justice, and reparation.

280. As documented through the testimonies collected for this report, the harm caused by surveillance extends far beyond the initial violation of privacy. Victims live in a permanent state of uncertainty, not knowing what information was extracted from their devices, how it might be used against them or their contacts, or whether the surveillance continues. This ongoing uncertainty creates lasting psychological harm and prevents individuals from moving forward with their lives and work.

281. The Special Rapporteurship emphasizes that addressing impunity for surveillance abuses requires more than prosecution of perpetrators—though such prosecutions are essential. It requires recognition of the specific harm caused to individuals, provision of complete information about the scope and duration of surveillance, destruction of illegally obtained data, and guarantees that such violations will not be repeated.

282. The transnational nature of surveillance operations, facilitated by commercial spyware companies and enabled by inadequate legal frameworks, has created jurisdictional gaps that further exacerbate impunity. Victims of surveillance frequently cannot obtain remedy in domestic courts and face insurmountable barriers when seeking accountability across borders.

283. The evidence presented in this report demonstrates that incremental reforms and voluntary industry initiatives have proven inadequate to address the systematic nature of surveillance abuses. The scale and persistence of documented violations, the failure of existing accountability mechanisms, and the continued expansion of surveillance capabilities across the region require nothing short of systemic transformation of how surveillance technologies are developed, deployed, and governed.

284. The SRFOE concludes that effective reform must address not only the symptoms of surveillance abuse but its structural causes, including the commercial incentives that drive surveillance

proliferation, the legal frameworks that enable excessive state surveillance powers, and the institutional failures that perpetuate impunity for surveillance violations.

285. In relation to the observations and conclusions presented in this report, and with basis in the powers conferred by Article 41.b of the American Convention on Human Rights, the Special Rapporteurship formulates the following recommendations:

To OAS Member States:

1. Develop an OAS-based regional strategy for addressing the human rights impacts of digital surveillance technologies in the region, including the following elements:
    a. Establish a specialized OAS working group to lead the aforementioned initiatives.
    b. Develop region-specific standards and principles regarding the use and procurement of surveillance technologies by states, as well as the transparency, oversight, and accountability, drawing on Inter-American jurisprudence and international best practices.
    c. Initiate and lead a dialogue among OAS member states, civil society, and other stakeholders, including engagement with the PEGA committee recommendations, the Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware, and other multilateral initiatives.

2. Review and update legal frameworks governing surveillance to ensure compliance with international human rights law. In particular: (i) strengthen judicial authorization and oversight mechanisms; (ii) establish protections for human rights defenders, journalists, activists and lawyers, including anti-SLAPP measures and whistleblower protections; (iii) require transparency in surveillance procurement and deployment; and (iv) provide notification mechanisms for individuals subjected to surveillance.

3. Establish legal mechanisms to ensure effective remedies for victims of surveillance abuses, including provisions to address evidentiary challenges and jurisdictional gaps in digital surveillance cases.

4. Ensure comprehensive data protection legal frameworks with independent oversight authorities, applicable to both state and private actors including law enforcement and intelligence agencies, with specific mandates to review surveillance databases and predictive analysis systems for compliance with human rights standards.

5. Recognize biometric data as sensitive personal data and restrict government processing, including facial recognition systems, to proportionate uses with appropriate safeguards.

6. Adopt domestic legislative measures to give effect to the right to informational self-determination, allowing individuals' control over government collection, use, and retention of their personal data.

7. Ensure that digital ID systems and government digitization are designed in compliance with human rights standards and privacy safeguards.

8. Establish transparent processes for government decisions on software vulnerability disclosure that incorporate human rights considerations.

9. Implement procurement restrictions preventing state contracts with surveillance companies that violate human rights standards.

10. Enact, and work with other states in the region to coordinate sanctions against entities and individuals involved in surveillance abuses.

11. For those states that have not already signed on to the Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware, engage with the initiative in order to align its practices with human rights principles.

12. Prohibit, through the appropriate regulatory authority, the acquisition, import, and use of commercial spyware technologies lacking technical safeguards to limit functions to specific, necessary, and proportionate surveillance objectives.

13. Implement a human rights regulatory framework that governs surveillance activities that complies with international human rights law standards on privacy, due process, and judicial oversight to protect all persons under State jurisdiction. Until such a framework is implemented, establish a moratorium on the purchase, sale, transfer and use of all spyware.

14. Publicly commit to refrain from using targeted digital surveillance against human rights defenders, journalists and civil society from such surveillance and harassment.

15. Ensure that all legislation, regulatory reforms, and public policies include mandatory consultation processes with civil society organizations, victims of surveillance, and independent human rights experts.

16. In line with the UN Guiding Principles on Business and Human Rights, legally require companies to carry out appropriate human rights due diligence to identify the potential human rights impacts of all their products. The due diligence process must allow the company to determine whether technical safeguards could ensure its products are rights-respecting; if so, the company must immediately put them in place.

17. Adopt a ban on the use, development, production, sale and export of facial recognition technology for identification purposes by both state agencies and private sector actors.

To international community, financial institutions and investors:

18. Carry out human rights due diligence process when funding and incentivizing states' deployment of surveillance technologies, including assessment of judicial

oversight, privacy protections, and compliance with international human rights law.

19. Establish binding exclusionary criteria prohibiting funding and investment in surveillance projects and companies that lack adequate human rights safeguards, are linked to systematic violations, or develop mass surveillance technologies incompatible with international human rights law.

20. Provide funding and technical support to civil society organizations addressing human rights impacts of surveillance, including incident response, digital security training, and legal assistance for victims and at-risk communities.

To companies:

21. Implement comprehensive human rights due diligence processes that comply with the UN Guiding Principles on Business and Human Rights for all surveillance technology products and services. Such processes must assess the potential human rights impacts throughout the product lifecycle, including development, marketing, sale, and deployment phases, and must be conducted prior to market entry, updated regularly, and made publicly available in accessible formats.

22. Publish annual transparency reports that include: aggregate statistics on government requests for surveillance technology services; descriptions of due diligence processes and human rights safeguards implemented; information about technical capabilities and limitations of surveillance products; and documentation of any instances where services were denied due to human rights concerns.

23. Cooperate fully and proactively with criminal investigations and legal proceedings related to surveillance technology abuse by providing timely, complete, and accurate information to prosecutors, law enforcement authorities, and judicial bodies investigating violations of human rights through surveillance technologies.

24. Establish binding contractual human rights compliance requirements for all government and institutional clients that include: mandatory compliance with international human rights law in the use of surveillance technologies; prohibition on use against human rights defenders, journalists, lawyers, political opposition, and other protected groups except in accordance with judicial authorization and strict necessity and proportionality standards; requirements for regular reporting on surveillance deployment and compliance with human rights safeguards; and provisions allowing for immediate suspension of services and curtailing of confidentiality constraints upon evidence of human rights violations.

25. Implement notification protocols to inform targeted individuals when surveillance technologies targeting them have been deactivated or are no longer in use, including clear information about what data was collected, how it was used, whether it has been shared with third parties, and steps being taken to delete or anonymize the collected information.

26. Prohibit all business relationships with data brokers that collect, aggregate, or sell personal data for surveillance purposes, and establish contractual requirements that prevent government clients from supplementing surveillance technologies with commercially purchased personal data obtained without judicial authorization.

27. Establish independent technical auditing processes that allow qualified civil society organizations and human rights experts to examine surveillance technology capabilities and deployment protocols to verify compliance with human rights safeguards and contractual limitations on use.